BA

PATENT ABSTRACTS OF JAPAN

CORR. TO US 7,116,675

(11)Publication number : 2002-063084
(43)Date of publication of application : 28.02.2002

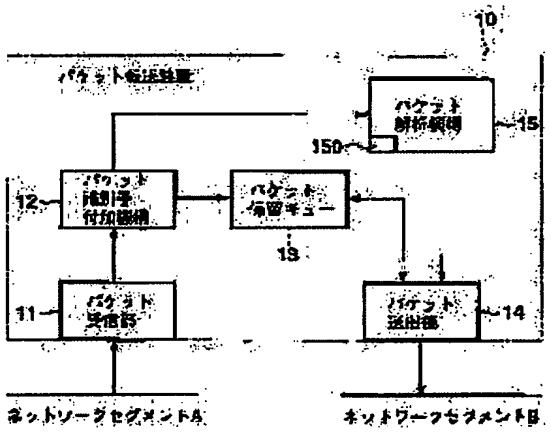
(51)Int.Cl. G06F 13/00
H04L 12/66
H04L 12/56

(21)Application number : 2000-249724
(22)Date of filing : 21.08.2000

(71)Applicant : TOSHIBA CORP
(72)Inventor : TATEOKA MASAMICHI

(54) PACKET-TRANSFERRING DEVICE, PACKET-TRANSFERRING METHOD, AND STORAGE MEDIUM STORED WITH PROGRAM THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a packet-transferring device and a packet-transferring method capable of realizing a packet-transferring device which does not allow a packet related to a fraudulant access to pass therethrough, without requiring a user to make a setting for judging whether to transfer the packet, and to provide a storage medium stored with a program therefor.
SOLUTION: A packet send-out mechanism 15 having received a packet from a packet identifier adding mechanism 12 sends out the packet, based on previously set information and determines whether the packet is related to fraudulant access.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－63084
（P2002－63084A）
(43)公開日　平成14年２月28日(2002.2.28)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ	５Ｂ０８９
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　11/20	Ｂ	５Ｋ０３０
12/56			１０２Ａ	

審査請求　有　　請求項の数35　ＯＬ　（全 28 頁）

(21)出願番号　特願2000－249724(P2000－249724)

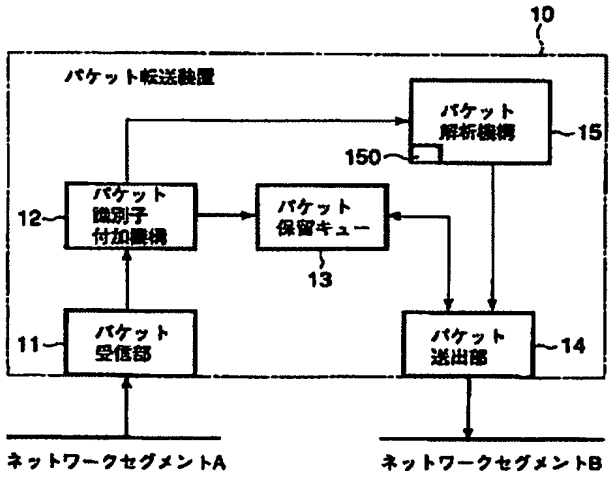
(22)出願日　平成12年８月21日(2000.8.21)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　楯岡　正道
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　5B089 GA04 GB01 HA04 KA17 KB13
5K030 GA15 HA08 JA05 KA03 KA13
KX13 KX24 KX30 LC01 LC15

(54)【発明の名称】　パケット転送装置、パケット転送方法、及びそのプログラムが格納された記憶媒体

(57)【要約】
【課題】本発明は、パケットを転送するか否かの判断を行なうための設定を利用者が行なうことなく、不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができるパケット転送装置、パケット転送方法、及びそのプログラムを格納した記憶媒体を提供することを課題とする。
【解決手段】パケット識別子付加機構１２からパケットを渡されたパケット送出機構１５は、当該パケットを予め設定された情報に基づいて送出し、当該パケットが不正アクセスに関わるか否かを判定する。



【特許請求の範囲】
【請求項１】　複数のネットワークセグメントの間に設けられ、ネットワークセグメント相互間で転送されるパケットを監視するパケット転送装置であって、
第１のネットワークセグメントを介して受信した受信パケットを第２のネットワークセグメントに送出する際に、予め設定された条件をもとに、前記受信パケットの情報に、前記第２のネットワークセグメントに接続された装置のソフトウェアに対し誤動作させる要因を含んでいるか否かを解析するパケット解析手段と、
前記解析手段によって前記誤動作させる要因を含んだ情報をもつ不正パケットであることを判定した際に、当該不正パケットを破棄し、正常なパケットと判定した受信パケットのみを前記第２のネットワークセグメントに送出する手段とを具備してなることを特徴とするパケット転送装置。
【請求項２】　少なくとも第１及び第２のネットワークセグメントに接続され、前記第１及び第２のネットワークセグメント相互の間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送装置に於いて、
前記第１のネットワークセグメントからのパケットを受信する受信手段と、
前記受信手段で受信した受信パケットに識別子を付加する識別子付加手段と、
前記識別子が付加された前記受信パケットを一時保留するパケット保留キューと、
前記受信パケットが予め設定した既知の誤動作条件を含む不正アクセスのパケットであるか否かを判定し、不正アクセスに関わるパケットで無いことを判定した際に、当該受信パケットの識別子を出力するパケット解析手段と、
前記パケット解析手段より出力された前記識別子を受信し、前記パケット保留キューから受信した前記識別子を持つ受信パケットを取り出し、前記第２のネットワークセグメントへ送出する送出手段とを具備することを特徴とするパケット転送装置。
【請求項３】　少なくとも３つ以上のネットワークセグメントに接続され、複数の前記ネットワークセグメント間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送装置に於いて、
前記ネットワークセグメントからのパケットを受信する受信手段と、
前記受信手段で受信した受信パケットに識別子を付加する識別子付加手段と、
前記識別子が付加された前記受信パケットを一時保留するパケット保留キューと、
前記受信パケットが予め設定した既知の誤動作条件を含む不正アクセスのパケットであるか否かを判定し、不正アクセスに関わるパケットで無いことを判定した際に、当該受信パケットの識別子を出力するパケット解析手段と、
前記パケット解析手段より出力された前記識別子を受信し、前記パケット保留キューから受信した前記識別子を持つ受信パケットを取り出し、当該受信パケットに含まれる宛先ＭＡＣアドレスから、送出すべきネットワークセグメントを判定する送出セグメント判定手段と、
前記送出セグメント判定手段によって判定されたネットワークセグメントへ当該受信パケットを送出する１つ又は複数の送出手段とを具備することを特徴とするパケット転送装置。
【請求項４】　少なくとも３つ以上のネットワークセグメントに接続され、複数の前記ネットワークセグメント間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送装置に於いて、
前記ネットワークセグメントからのパケットを受信する受信手段と、
前記受信手段で受信した受信パケットに識別子を付加する識別子付加手段と、
前記識別子が付加された前記受信パケットを送出先のネットワークセグメント毎に一時保留する複数のパケット保留キューと、
前記識別子が付加された前記受信パケットに含まれる宛先ＭＡＣアドレスから前記受信パケットの送出先ネットワークセグメントを判定し、当該ネットワークセグメントに対応する前記パケット保留キューに前記識別子が付加されたパケットを送出する送出セグメント判定手段と、
前記受信パケットが予め設定した既知の誤動作条件を含む不正アクセスのパケットであるか否かを判定し、不正アクセスに関わるパケットで無いことを判定した際に、当該受信パケットの前記識別子を出力するパケット解析手段と、
前記パケット保留キューに対応して設けられる複数の送出手段であって、前記パケット解析手段より出力された前記識別子を受信し、前記識別子を持つ受信パケットを保留している１つ又は複数の前記パケット保留キューから当該受信パケットを取り出し、対応付けられた前記ネットワークセグメントへ送出する送出手段とを具備することを特徴とするパケット転送装置。
【請求項５】　前記パケット解析手段は、過去に受信した不正アクセスに関わるパケットに含まれる文字列を記憶したデータベースを具備することを特徴とする請求項１または２または３または４記載のパケット転送装置。
【請求項６】　前記パケット転送装置に於いて、更に、前記パケット解析手段により不正アクセスに関わるパケットであると判定された場合、その不正パケットの存在、構造、形式、受信時刻、送信元の少なくともいずれ

かを含む詳細情報を取得して保持する不正アクセス履歴保持手段と、
前記不正アクセス履歴保持手段が保持する不正アクセス履歴を表示する不正アクセス履歴表示手段とを具備することを特徴とする請求項１または２または３または４記載のパケット転送装置。
【請求項７】　前記パケット転送装置に於いて、更に、
前記パケット解析手段によって不正パケットでないと判定された送出済みパケットを保持する送出済みパケット保持手段を設け、
前記パケット解析手段は不正パケットの解析時に、前記送出済みパケット保持手段に保持された前記送出済みパケットを参照することを特徴とする請求項１または２または３または４記載のパケット転送装置。
【請求項８】　前記パケット解析手段は、
前記受信パケットのヘッダ部のオプション、若しくはパラメータの組み合わせが、予め設定された既知の条件を満たしているか否かを判定する手段、
前記受信パケットが搬送しているデータの長さ、若しくはデータが指定するパラメータの組み合わせが、予め設定された既知の条件を満たしているか否かを判定する手段、
パケット相互のデータ構造、若しくはデータ内容が、予め設定された既知の条件を満たしているか否かを判定する手段の少なくとも一つの手段により、不正アクセスに関わるパケットであるか否かを判定することを特徴とする請求項１または２または３または４記載のパケット転送装置。
【請求項９】　前記パケット解析手段は、
前記識別子が付加された受信パケットを格納するパケット格納手段と、
不正アクセスのパケットに含まれる文字列を一部に内蔵するパケット解析プログラムが格納されるプログラム格納手段と、
前記パケット解析プログラムに基づき、前記パケット格納手段に格納された受信パケットについて、既知の誤動作条件を含む不正アクセスのパケットであるか否かを判定し、不正アクセスに関わるパケットで無いことを判定した際に、当該受信パケットの識別子を出力するプログラム実行手段とを具備することを特徴とする請求項１または２または３または４記載のパケット転送装置。
【請求項１０】　前記パケット転送装置は、更に、
前記プログラム格納手段に格納された前記パケット解析プログラムを更新する解析プログラム更新手段を具備することを特徴とする請求項９記載のパケット転送装置。
【請求項１１】　前記解析プログラム更新手段は、
シリアルインタフェース、若しくはネットワークインタフェースでなる通信インタフェースと、
前記通信インタフェースを介して受信したデータから、解析プログラム更新指示を示す特定の形式を満たしていることを識別する解析プログラム更新指示形式の識別手段とを具備し、
前記解析プログラム更新指示形式の識別手段が前記解析プログラム更新指示であると識別したデータをもとに、前記パケット解析プログラムをロード、若しくは更新することを特徴とする請求項１０記載のパケット転送装置。
【請求項１２】　前記解析プログラム更新手段は、
前記受信手段で受信したパケットから、前記パケット解析プログラムの更新指示を示す特定の形式を満たしているデータであることを識別する解析プログラム更新指示形式の識別手段を具備し、
前記解析プログラム更新指示形式の識別手段が前記解析プログラム更新指示であると識別した受信パケットのデータをもとに、前記パケット解析プログラムをロードし、若しくは更新することを特徴とする請求項１０記載のパケット転送装置。
【請求項１３】　前記解析プログラム更新指示形式の識別手段は、
前記パケット内のデータ、若しくは前記シリアルインタフェースを介して入力されたデータ、若しくは前記ネットワークインタフェースを介して入力されたデータから、電子署名情報を抽出し、当該電子署名情報が正当な署名であるか否かを判定し、正当であると判定した場合、前記パケット解析プログラムをロードし、若しくは更新することを特徴とする請求項１２記載のパケット転送装置。
【請求項１４】　前記パケット転送装置は、更に、
前記パケット解析手段が不正アクセスに関わるパケットであると判定した場合、その不正パケットの存在、構造、形式、受信時刻、送信元等の少なくともいずれかを含む詳細情報を他の装置に通知する装置内情報通知手段を具備することを特徴とする請求項１または２または３または４記載のパケット転送装置。
【請求項１５】　前記パケット解析プログラムの設定または更新に伴う通信、若しくは不正パケットの前記詳細情報を他の装置に通知する通信である特定通信のみに使用する送信元アドレスを予め設定する通信用アドレス設定手段と、前記通信用アドレス設定手段により設定された通信用アドレスを保持する通信用アドレス保持手段と、
前記特定通信を行わないときは、前記送信元アドレス宛てに送られるパケットを破棄し、前記特定通信を行うときのみ、前記送信元アドレス宛てのパケットを受信する通信制御手段とを具備してなることを特徴とする請求項１０または１４記載のパケット転送装置。
【請求項１６】　前記パケット解析プログラムの設定または更新に伴う通信、若しくは不正パケットの前記詳細情報を他の装置に通知する通信である特定通信のみに使用する送信元アドレスとして、当該特定通信の送出先ネ

ットワークセグメントとは異なるネットワークセグメントから過去に受信したパケットの送信元アドレスの１つを選択する通信用アドレス選択手段と、
前記通信用アドレス選択手段で選択された送信元アドレスを宛先としたパケットのうち、当該特定通信に関わるパケットを横奪するパケット横奪手段とを具備することを特徴とする請求項１０または１４記載のパケット転送装置。
【請求項１７】　転送対象であるパケットから前記特定通信の開始指示である特定の形式を満たしているデータであることを識別して、前記特定通信を開始する通信開始指示形式識別手段を具備することを特徴とする請求項１５または１６記載のパケット転送装置。
【請求項１８】　前記通信開始指示形式識別手段は、データ中に含まれている電子署名が正当な署名であるか否かを判定し、正当な署名であると判定した場合のみ当該データを通信開始指示であると識別する電子署名識別手段を具備することを特徴とする請求項１７記載のパケット転送装置。
【請求項１９】　複数のネットワークセグメントの間に設けられ、ネットワークセグメント相互間で転送されるパケットを監視するパケット転送装置であって、
第１のネットワークセグメントより受信した受信パケットを第２のネットワークセグメントに送出する際に、予め設定された条件をもとに、前記受信パケットの情報に、前記第２のネットワークセグメントに接続される装置のソフトウェアに対し誤動作させる要因を含んでいるか否かを判定し、
前記誤動作させる要因を含んだ情報をもつ不正パケットであることを判定した際に、当該不正パケットを破棄し、正常なパケットと判定した受信パケットを前記第２のネットワークセグメントに送出することを特徴とするパケット転送方法。
【請求項２０】　少なくとも第１及び第２のネットワークセグメントに接続され、前記第１及び第２のネットワークセグメント相互の間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送方法に於いて、
前記第１のネットワークセグメントからのパケットを受信するステップと、
前記受信した受信パケットに識別子を付加するステップと、
前記識別子が付加された前記受信パケットを一時保留するステップと、
前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定し、判定した正常な受信パケットの前記識別子を出力するステップと、
前記識別子を受信し、前記一時保留されている前記受信パケットの中から、受信した前記識別子を持つ前記受信パケットを取り出し、前記第２のネットワークセグメントに送出するステップとを具備することを特徴とするパケット転送方法。
【請求項２１】　少なくとも３つ以上のネットワークセグメントに接続され、複数の前記ネットワークセグメント間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送方法に於いて、
前記ネットワークセグメントの一つからパケットを受信するステップと、
前記受信した受信パケットに識別子を付加するステップと、
前記識別子が付加された前記受信パケットを一時保留するステップと、
前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定し、判定した正常な受信パケットの前記識別子を出力するステップと、
前記識別子を受信し、前記一時保留されている前記受信パケットの中から、受信した前記識別子を持つ前記受信パケットを取り出し、当該受信パケットに含まれるＭＡＣアドレスから送出すべきネットワークセグメントを判定するステップと、
前記判定されたネットワークセグメントに対し、取り出した前記受信パケットを送出するステップとを具備することを特徴とするパケット転送方法。
【請求項２２】　少なくとも３つ以上のネットワークセグメントに接続され、複数の前記ネットワークセグメント間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送方法に於いて、
前記ネットワークセグメントの一つからパケットを受信するステップと、
前記受信した受信パケットに識別子を付加するステップと、
前記識別子が付加された前記受信パケットに含まれる宛先ＭＡＣアドレスから当該受信パケットの送出先ネットワークセグメントを判定し、前記送出先のネットワークセグメント毎に設けられた一時保留キューに、前記判定に従って前記受信パケットを格納するステップと、
前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定し、判定した正常な受信パケットの前記識別子を出力するステップと、
前記識別子を受信し、前記一時保留キューの前記受信パケットの中から、受信した前記識別子を持つ前記受信パケットを取り出し、対応するネットワークセグメントに送出するステップとを具備することを特徴とするパケット転送方法。
【請求項２３】　前記パケット転送方法に於いて、更

に、
不正アクセスに関わるパケットであると判定したパケットの受信時刻、若しくは送信元を少なくとも含む詳細情報を記録するするステップと、
当該記録された詳細情報を表示するステップとを有してなる請求項１９または２０または２１または２２記載のパケット転送方法。
【請求項２４】　前記パケット転送方法に於いて、更に、
前記正常なパケットと判定され、過去に送出済み受信パケットを保持する送出済みパケット保持手段を設け、
前記パケット解析時に、前記パケット保持手段に格納された前記送出済み受信パケットを参照して、不正アクセスに関わるパケットであるか否かの判定を行なうステップを有することを特徴とする請求項１９または２０または２１または２２記載のパケット転送方法。
【請求項２５】　前記パケット転送方法に於いて、更に、
前記識別子が付加された受信パケットを格納するパケット格納手段と、不正アクセスのパケットに含まれる文字列を一部に内蔵するパケット解析プログラムが格納されるプログラム格納手段と、前記パケット解析プログラムを実行するプログラム実行手段とを設け、
前記受信パケットの解析時に、プログラム実行手段は、前記パケット解析プログラムに基づき、前記パケット格納手段に格納された受信パケットについて、既知の誤動作条件を含む不正アクセスのパケットであるか否かを判定し、不正アクセスに関わるパケットで無いことを判定した際に、当該受信パケットの識別子を出力することを特徴とする請求項２０または２１または２２記載のパケット転送方法。
【請求項２６】　前記パケット転送方法に於いて、更に、
シリアルインタフェース、若しくは前記ネットワークインタフェース、若しくは独立したネットワークインタフェースを介して前記パケット解析プログラムの更新指示のデータを受信するステップと、
受信したデータが前記パケット解析プログラムの更新指示を示す特定の形式を満たしていることを識別できた時に、前記パケット解析プログラムを更新するステップとを有してなることを特徴とする請求項２５記載のパケット転送方法。
【請求項２７】　前記パケット転送方法に於いて、
前記パケット解析プログラムの更新指示を示す特定の形式を満たしていることを識別するために、前記受信したデータ中に含まれている電子署名が正当な署名であるか否かを判定することを特徴とする請求項２６記載のパケット転送方法。
【請求項２８】　前記パケット転送方法に於いて、更に、
不正アクセスに関わるパケットであると判定したパケットの受信時刻、送信元の少なくともいずれかを含む詳細情報を記録するするステップと、
当該記録された詳細情報を他の装置に通知するステップとを具備することを特徴とする請求項１９または２０または２１または２２記載のパケット転送方法。
【請求項２９】　前記パケット転送方法に於いて、更に、
前記パケット解析プログラムの更新に伴う通信や、装置内の情報を他の装置に対して通知する通信などの特定通信を行なう際に使用する送信元アドレスを、予め設定するステップを具備し、
前記特定通信を行なう間のみ、前記送信元アドレス宛のパケットを受信し、
前記特定通信を行なっていない間は、前記送信元アドレス当てのパケットを破棄することを特徴とする請求項２６または２８記載のパケット転送方法。
【請求項３０】　前記パケット転送方法に於いて、更に、
前記パケット解析プログラムの更新に伴う通信や、装置内の情報を他の装置に対して通知する通信などの特定通信を行なう際に使用する送信元アドレスを、送信先ネットワークセグメントとは異なるネットワークセグメントから、過去に受信したパケットの送信元アドレスの一つを、当該通信を行なう際の送信元アドレスとして、予め選択するステップを具備し、
前記特定通信を行なう間のみ、前記送信元アドレス宛ての通信に関わるパケットを横奪し、
前記特定通信を行なっていない間は、前記送信元アドレス宛てのパケットは転送処理を行なうことを特徴とする請求項２６または２８記載のパケット転送方法。
【請求項３１】　前記パケット転送方法に於いて、前記受信パケットが不正アクセスに関わるパケットであると判定する条件は、
前記受信パケットのヘッダフィールドのオプション、若しくはパラメータの組み合わせが、パケット送出先に誤動作を引き起こす可能性があるとして予め設定された既知の条件を満たしているとき、
又は、前記受信パケットが搬送しているデータの長さ、若しくはデータが指定するパラメータの組み合わせが、当該データを処理するソフトウェアに誤動作を引き起こす可能性があるとして予め設定された既知の条件を満たしているとき、
又は、前記受信パケット相互のデータ構造、若しくはデータ内容が、パケット送出先に誤動作を引き起こす可能性があるとして予め設定された既知の条件を満たしているとき、
のいずれかであることを特徴とする請求項１９または２０または２１または２２記載のパケット転送方法。
【請求項３２】　少なくとも２つ以上のネットワークセ

グメント相互の間で転送されるパケットを監視するパケット転送装置に記憶され、
前記ネットワークセグメントの一方からのパケットを受信する機能と、
前記受信した受信パケットに識別子を付加する機能と、
前記識別子が付加された前記受信パケットを一時保留する機能と、
前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定した際に、当該受信パケットの識別子を出力する機能と、
前記識別子を受信し、前記一時保留されているパケットの中から受信した前記識別子を持つ受信パケットを取り出し、送出先の他方のネットワークセグメントへ送出する機能とを実現するためのプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。
【請求項３３】　少なくとも３つ以上のネットワークセグメント間で転送されるパケットを監視するパケット転送装置に記憶され、
前記ネットワークセグメントの一つからパケットを受信する機能と、
前記受信した受信パケットに識別子を付加する機能と、
前記識別子が付加された前記受信パケットを一時保留する機能と、
前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定した際に、当該受信パケットの識別子を出力する機能と、
前記識別子を受信し、前記一時保留されている受信パケットの中から受信した前記識別子を持つ受信パケットを取り出し、当該受信パケットに含まれるＭＡＣアドレスから送出すべきネットワークセグメントを判定する機能と、
前記判定されたネットワークセグメントへ当該受信パケットを送出する機能とを実現するためのプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。
【請求項３４】　少なくとも３つ以上のネットワークセグメント間で転送されるパケットを監視するパケット転送装置に記憶され、
前記ネットワークセグメントの一つからパケットを受信する機能と、
前記受信した受信パケットに識別子を付加する機能と、
前記識別子が付加された前記受信パケットに含まれるＭＡＣアドレスから、送出すべきネットワークセグメントを判定する機能と、
前記識別子が付加された前記受信パケットを、前記判定された送出先ネットワークセグメント毎に分けて一時保留する機能と、
前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定した際に、当該受信パケットの識別子を出力する機能と、
前記識別子を受信し、前記一時保留されている前記受信パケットの中から、受信した前記識別子を持つ受信パケットを取り出し、当該受信パケットを、前記判定された送出先ネットワークセグメントへ送出する機能とを実現するためのプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。
【請求項３５】　前記受信パケットを解析し、不正アクセスに関わるパケットであるか否かを判定する機能を実現するプログラムに、
予め設定された既知の条件をもとに、前記受信パケットのヘッダフィールドのオプション、若しくはパラメータの組み合わせが、パケット送出先に誤動作を引き起こす可能性のある不正アクセスに関わるパケットを判定する機能、
予め設定された既知の条件をもとに、前記受信パケットが搬送しているデータの長さ、若しくはデータが指定するパラメータの組み合わせが、当該データを処理するソフトウェアに誤動作を引き起こす可能性のある不正アクセスに関わるパケットを判定する機能、
予め設定された既知の条件をもとに、前記受信パケット相互のデータ構造、若しくはデータ内容が、パケット送出先に誤動作を引き起こす可能性のある不正アクセスに関わるパケットを判定する機能、
の少なくとも一つ以上の機能が組み込まれた請求項３２または３３または３４記載のコンピュータ読み取り可能な記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、複数のネットワークセグメント相互の間でパケットを転送するパケット転送装置、パケット転送方法、及びそのプログラムが格納された記憶媒体に関する。
【０００２】
【従来の技術】従来、複数のネットワークセグメント相互の間に接続されて、これらセグメント間でパケットを転送するパケット転送装置に於いて、不正アクセスを防止するための、パケットを転送するか否の判断は、利用者がネットワーク若しくは他の設定手段を用いて設定した、宛先／送信元のネットワークアドレスやサービス番号等により行っていた。
【０００３】この際の従来のパケット転送装置に於ける不正アクセス防止手段を図２２乃至図２４を参照して説明する。従来のパケット転送装置の構成例を図２２に示している。ここでは、パケット転送装置０１の構成要素として、送信元となる一方のネットワークセグメントからのパケットを受信するパケット受信部０２、パケット受信部０２で受信したパケットをフィルタリング（選定）制御するパケットフィルタ部０３、パケットフィルタ部０３を通過したパケットを送出先となる他方のネットワークセグメントに送出するパケット送出部０４、不正アクセスを防止するための宛先／送信元のネットワー

クアドレスやサービス番号等を設定するルール設定部０５、ルール設定部０５で設定されたアドレス等の情報を保持しパケットフィルタ部０３が参照するルール保持部０６等が設けられる。

【０００４】上記構成によるパケット転送装置０１を含むネットワークシステムの一構成例を図２３に示し、パケット転送装置０１のルール保持部０６に格納される内容例を図２４に示している。

【０００５】利用者は、ネットワークを介し、ルール設定部０５の機能を用いて、ルール保持部０６に、宛先／送信元ネットワークアドレス、サービス番号、転送を許可するか否かの識別情報等を予め設定しておく。

【０００６】ここでは上記図２２に示す構成のパケット転送装置０１を用いて上記図２３に示すようなネットワークシステムが構築され、利用者がルール設定部０５の機能を用いて図２４に示すような設定内容（ルール）が予めルール保持部０６に保持しているものとする。

【０００７】その状態で、例えば、ネットワークアドレスとして、［１９２．１６８．１．１２］を持つホストから、［１９２．１６８．０．３１］を持つホストのＨＴＴＰサービスを利用しようとするパケットがパケット受信部０２で受信されたとする。

【０００８】この受信パケットは、パケットフィルタ部０３に送られる。

【０００９】パケットフィルタ部０３では、ルール保持部０６に格納された、予め利用者が設定した図２４に示すようなルールを参照する。

【００１０】ここでパケットフィルタ部０３は、図２４に示すルールを参照して、ネットワークアドレスとして、［１９２．１６８．１．１２］を持つホストから、［１９２．１６８．０．３１］を持つホストのＨＴＴＰサービスを利用するアクセスは許可されていることを判断し、上記パケットをパケット送出部０４に送出する。そして、パケット送出部０４からネットワークアドレスとして、［１９２．１６８．０．３１］のアドレスを持つホストへ転送され、通信が完了する。

【００１１】また、例えば、ネットワークアドレスとして、［１９２．１６８．１．１３］を持つホストから、［１９２．１６８．０．３１］を持つホストのＨＴＴＰサービスを利用しようとするパケットがパケット受信部０２で受信されたとすると、その受信パケットは、パケットフィルタ部０３に送られる。

【００１２】パケットフィルタ部０３では、ルール保持部０６に格納された、利用者が予め設定した図２４に示すルールを参照する。

【００１３】ここでパケットフィルタ部０３は、図２４に示すルールを参照すると、ネットワークアドレスとして、［１９２．１６８．１．１３］を持つホストから、［１９２．１６８．０．３１］を持つホストのＨＴＴＰサービスを利用するアクセスは不許可とされていることを判断する。したがって、このパケットはパケットフィルタ部０３によって不正アクセスと判断し破棄され、パケット送出部０４からは上記受信したパケットが送出されないこととなる。

【００１４】他の宛先／送信元／サービスの各パケットに関しても、上記同様に、図２４に示すルール保持部０６の内容（ルール）に従って、送出／破棄が行なわれる。

【００１５】上述した従来のパケット転送装置に於ける不正アクセス防止手段には、宛先／送信元のＭＡＣ（Media Access Control）アドレスや、さらに上位のプロトコルの宛先／送信元アドレスやサービス番号等によって、パケットを転送するか否かを判断するだけでは、転送するように設定されたアドレスやサービス番号を用いた不正アクセスは防止できず、不正アクセスに関わるパケットを通過させないという目的には、不十分であるという問題があった。

【００１６】例えば、宛先／送信元ＭＡＣアドレスや、さらに上位のプロトコルの宛先／送信元アドレスやサービス番号等がすべて正しく設定されていたとしても、その設定された送信元を介して（経由して）不正アクセスと見做されるデータをもつパケットが転送され、当該パケットで搬送されたデータにより、受信側システムのアプリケーション等が侵害されてしまうという、信頼性の問題があった。

【００１７】また、パケットを転送するか否かの判断を行なうための宛先／送信元ＭＡＣアドレスや、さらに上位のプロトコルの宛先／送信元アドレスやサービス番号等の設定は、利用者や設置場所毎に異なるため、パケット転送装置の設置に伴って、設定を行なう必要があったが、この設定は、比較的困難であり、しばしば誤った設定がなされ、不正アクセスを許してしまうという問題もあった。

【００１８】また、設定をネットワーク経由で行なうにはＩＰアドレス等のネットワークアドレスが必要であり、それは、逆に不正アクセスの対象となり得るという問題もあった。

【００１９】また、宛先／送信元ＭＡＣアドレスや、さらに上位のプロトコルの宛先／送信元アドレスやサービス番号等によって、転送しないと判断するパケットが到着したとしても、それが、必ずしも不正アクセスとは言い切れず、したがって、転送しないと判断するパケットが到着したことを何らかの形で表示したとしても、不正アクセスがなされていることの表示とはならないという問題もあった。

【００２０】

【発明が解決しようとする課題】上述したように、従来のパケット転送装置に於ける不正アクセス防止手段に於いては、宛先／送信元のＭＡＣアドレスや、さらに上位のプロトコルの宛先／送信元アドレスやサービス番号等

によって、パケットを転送するか否かを判断するだけでは、転送するように設定されたアドレスやサービス番号を用いた不正アクセスは防止できず、不正アクセスに関わるパケットを通過させないという目的には、不十分であるという問題があった。

【００２１】また、パケットを転送するか否かの判断を行なうための宛先／送信元ＭＡＣアドレスや、さらに上位のプロトコルの宛先／送信元アドレスやサービス番号等の設定は、利用者や設置場所毎に異なるため、パケット転送装置の設置に伴って、設定を行なう必要があったが、この設定は、比較的困難であり、しばしば誤った設定がなされ、不正アクセスを許してしまうという問題もあった。

【００２２】また、設定をネットワーク経由で行なうには、ＩＰアドレス等のネットワークアドレスが必要であり、それは、逆に不正アクセスの対象となり得るという問題もあった。

【００２３】更に、宛先／送信元ＭＡＣアドレスや、さらに上位のプロトコルの宛先／送信元アドレスやサービス番号等によって、転送しないと判断するパケットが到着したとしても、それが、必ずしも不正アクセスとは言い切れず、したがって、転送しないと判断するパケットが到着したことを何らかの形で表示したとしても、不正アクセスがなされていることの表示とはならないという問題もあった。

【００２４】このように、従来のパケット転送装置に於いては、不正アクセス防止に関して、信頼性の面で種々の問題があるとともに、利用者にかかる作業負担が大きいという問題があった。

【００２５】本発明は上記実情に鑑みなされたもので、利用者に大きな作業負担をかけることなく、信頼性の高い不正アクセスの防止機能を実現できるパケット転送装置、パケット転送方法、及びそのプログラムが格納された記憶媒体を提供することを目的とする。

【００２６】また本発明は、送信元より転送されたパケット（受信パケット）の内容を送出して不正アクセスに関わるパケットでないことを判定する機能をもつことで、不正アクセスに関わるパケットの転送を確実に防止することのできる、信頼性の高い不正アクセスの防止機能が実現できるパケット転送装置、パケット転送方法、及びそのプログラムが格納された記憶媒体を提供することを目的とする。

【００２７】また本発明は、宛先／送信元ＭＡＣアドレスや、上位のプロトコルの宛先／送信元アドレスや、サービス番号等によって、受信パケットを転送するか否かを判断するだけでは防止できない不正アクセスに関わるパケットを通過させないパケット転送機構、パケットを転送するか否かの判断を行なうための設定を利用者が行なうことなく不正アクセスに関わるパケットを通過させないパケット転送機構、自身が不正アクセスの対象となることを防ぐことのできるパケット転送機構、不正アクセスが為されていることを表示可能なパケット転送機構、等を容易に実現することのできるパケット転送装置、パケット転送方法、及びそのプログラムが格納された記憶媒体を提供することを目的とする。

【００２８】

【課題を解決するための手段】上記目的を達成するために本発明のパケット転送装置は、複数のネットワークセグメントの間に設けられ、ネットワークセグメント相互間で転送されるパケットを監視するパケット転送装置であって、第１のネットワークセグメントを介して受信した受信パケットを第２のネットワークセグメントに送出する際に、予め設定された条件をもとに、前記受信パケットの情報に、前記第２のネットワークセグメントに接続された装置のソフトウェアに対し誤動作させる要因を含んでいるか否かを解析するパケット解析手段と、前記解析手段によって前記誤動作させる要因を含んだ情報をもつ不正パケットであることを判定した際に、当該不正パケットを破棄し、正常なパケットと判定した受信パケットのみを前記第２のネットワークセグメントに送出する手段とを具備してなることを特徴とする。

【００２９】また本発明の装置は、少なくとも第１及び第２のネットワークセグメントに接続され、前記第１及び第２のネットワークセグメント相互の間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送装置に於いて、前記第１のネットワークセグメントからのパケットを受信する受信手段と、前記受信手段で受信した受信パケットに識別子を付加する識別子付加手段と、前記識別子が付加された前記受信パケットを一時保留するパケット保留キューと、前記受信パケットが予め設定した既知の誤動作条件を含む不正アクセスのパケットであるか否かを判定し、不正アクセスに関わるパケットで無いことを判定した際に、当該受信パケットの識別子を出力するパケット解析手段と、前記パケット解析手段より出力された前記識別子を受信し、前記パケット保留キューから受信した前記識別子を持つ受信パケットを取り出し、前記第２のネットワークセグメントへ送出する送出手段とを具備することを特徴とする。

【００３０】また本発明の装置は、少なくとも３つ以上のネットワークセグメントに接続され、複数の前記ネットワークセグメント間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送装置に於いて、前記ネットワークセグメントからのパケットを受信する受信手段と、前記受信手段で受信した受信パケットに識別子を付加する識別子付加手段と、前記識別子が付加された前記受信パケットを一時保留するパケット保留キューと、前記受信パケットが予め設定した既知の誤動作条件を含む不正アクセスのパケットであるか否かを判定し、不正アクセ

スに関わるパケットで無いことを判定した際に、当該受信パケットの識別子を出力するパケット解析手段と、前記パケット解析手段より出力された前記識別子を受信し、前記パケット保留キューから受信した前記識別子を持つ受信パケットを取り出し、当該受信パケットに含まれる宛先ＭＡＣアドレスから、送出すべきネットワークセグメントを判定する送出セグメント判定手段と、前記送出セグメント判定手段によって判定されたネットワークセグメントへ当該受信パケットを送出する１つ又は複数の送出手段とを具備することを特徴とする。

【００３１】また本発明の装置は、少なくとも３つ以上のネットワークセグメントに接続され、複数の前記ネットワークセグメント間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送装置に於いて、前記ネットワークセグメントからのパケットを受信する受信手段と、前記受信手段で受信した受信パケットに識別子を付加する識別子付加手段と、前記識別子が付加された前記受信パケットを送出先のネットワークセグメント毎に一時保留する複数のパケット保留キューと、前記識別子が付加された前記受信パケットに含まれる宛先ＭＡＣアドレスから前記受信パケットの送出先ネットワークセグメントを判定し、当該ネットワークセグメントに対応する前記パケット保留キューに前記識別子が付加されたパケットを送出する送出セグメント判定手段と、前記受信パケットが予め設定した既知の誤動作条件を含む不正アクセスのパケットであるか否かを判定し、不正アクセスに関わるパケットで無いことを判定した際に、当該受信パケットの前記識別子を出力するパケット解析手段と、前記パケット保留キューに対応して設けられる複数の送出手段であって、前記パケット解析手段より出力された前記識別子を受信し、前記識別子を持つ受信パケットを保留している１つ又は複数の前記パケット保留キューから当該受信パケットを取り出し、対応付けられた前記ネットワークセグメントへ送出する送出手段とを具備することを特徴とする。

【００３２】また本発明の装置は、過去に受信した不正アクセスに関わるパケットに含まれる文字列を記憶したデータベースを具備することを特徴とする。

【００３３】また本発明の装置は、前記パケット解析手段により不正アクセスに関わるパケットであると判定された場合、その不正パケットの存在、構造、形式、受信時刻、送信元の少なくともいずれかを含む詳細情報を取得して保持する不正アクセス履歴保持手段と、前記不正アクセス履歴保持手段が保持する不正アクセス履歴を表示する不正アクセス履歴表示手段とを具備することを特徴とする。

【００３４】また本発明の装置は、前記パケット解析手段によって不正パケットでないと判定された送出済みパケットを保持する送出済みパケット保持手段を設け、前記パケット解析手段は不正パケットの解析時に、前記送出済みパケット保持手段に保持された前記送出済みパケットを参照することを特徴とする。

【００３５】また本発明の装置は、前記受信パケットのヘッダ部のオプション、若しくはパラメータの組み合わせが、予め設定された既知の条件を満たしているか否かを判定する手段、前記受信パケットが搬送しているデータの長さ、若しくはデータが指定するパラメータの組み合わせが、予め設定された既知の条件を満たしているか否かを判定する手段、パケット相互のデータ構造、若しくはデータ内容が、予め設定された既知の条件を満たしているか否かを判定する手段、の少なくとも一つの手段により、不正アクセスに関わるパケットであるか否かを判定することを特徴とする。

【００３６】また本発明の装置は、前記識別子が付加された受信パケットを格納するパケット格納手段と、不正アクセスのパケットに含まれる文字列を一部に内蔵するパケット解析プログラムが格納されるプログラム格納手段と、前記パケット解析プログラムに基づき、前記パケット格納手段に格納された受信パケットについて、既知の誤動作条件を含む不正アクセスのパケットであるか否かを判定し、不正アクセスに関わるパケットで無いことを判定した際に、当該受信パケットの識別子を出力するプログラム実行手段とを具備することを特徴とする。

【００３７】また本発明の装置は、前記プログラム格納手段に格納された前記パケット解析プログラムを更新する解析プログラム更新手段を具備することを特徴とする。

【００３８】また本発明の装置は、前記パケット転送装置に於いて、シリアルインタフェース、若しくはネットワークインタフェースでなる通信インタフェースと、前記通信インタフェースを介して受信したデータから、解析プログラム更新指示を示す特定の形式を満たしていることを識別する解析プログラム更新指示形式の識別手段とを具備し、前記解析プログラム更新指示形式の識別手段が前記解析プログラム更新指示であると識別したデータをもとに、前記パケット解析プログラムをロード、若しくは更新することを特徴とする。

【００３９】また本発明の装置は、前記受信手段で受信したパケットから、前記パケット解析プログラムの更新指示を示す特定の形式を満たしているデータであることを識別する解析プログラム更新指示形式の識別手段を具備し、前記解析プログラム更新指示形式の識別手段が前記解析プログラム更新指示であると識別した受信パケットのデータをもとに、前記パケット解析プログラムをロードし、若しくは更新することを特徴とする。

【００４０】また本発明の装置は、前記パケット内のデータ、若しくは前記シリアルインタフェースを介して入力されたデータ、若しくは前記ネットワークインタフェースを介して入力されたデータから、電子署名情報を抽

出し、当該電子署名情報が正当な署名であるか否かを判定し、正当であると判定した場合、前記パケット解析プログラムをロードし、若しくは更新することを特徴とする。

【００４１】また本発明の装置は、前記パケット解析手段が不正アクセスに関わるパケットであると判定した場合、その不正パケットの存在、構造、形式、受信時刻、送信元等の少なくともいずれかを含む詳細情報を他の装置に通知する装置内情報通知手段を具備することを特徴とする。

【００４２】また本発明の装置は、前記パケット解析プログラムの設定または更新に伴う通信、若しくは不正パケットの前記詳細情報を他の装置に通知する通信である特定通信のみに使用する送信元アドレスを予め設定する通信用アドレス設定手段と、前記通信用アドレス設定手段により設定された通信用アドレスを保持する通信用アドレス保持手段と、前記特定通信を行わないときは、前記送信元アドレス宛てに送られるパケットを破棄し、前記特定通信を行うときのみ、前記送信元アドレス宛てのパケットを受信する通信制御手段とを具備してなることを特徴とする。

【００４３】また本発明の装置は、前記パケット解析プログラムの設定または更新に伴う通信、若しくは不正パケットの前記詳細情報を他の装置に通知する通信である特定通信のみに使用する送信元アドレスとして、当該特定通信の送出先ネットワークセグメントとは異なるネットワークセグメントから過去に受信したパケットの送信元アドレスの１つを選択する通信用アドレス選択手段と、前記通信用アドレス選択手段で選択された送信元アドレスを宛先としたパケットのうち、当該特定通信に関わるパケットを横奪するパケット横奪手段とを具備することを特徴とする。

【００４４】また本発明の装置は、転送対象であるパケットから前記特定通信の開始指示である特定の形式を満たしているデータであることを識別して、前記特定通信を開始する通信開始指示形式識別手段を具備することを特徴とする。

【００４５】また本発明の装置は、前記通信開始指示形式識別手段は、データ中に含まれている電子署名が正当な署名であるか否かを判定し、正当な署名であると判定した場合のみ当該データを通信開始指示であると識別する電子署名識別手段を具備することを特徴とする。

【００４６】上記目的を達成するために、本発明のパケット転送方法は、複数のネットワークセグメントの間に設けられ、ネットワークセグメント相互間で転送されるパケットを監視するパケット転送装置であって、第１のネットワークセグメントより受信した受信パケットを第２のネットワークセグメントに送出する際に、予め設定された条件をもとに、前記受信パケットの情報に、前記第２のネットワークセグメントに接続される装置のソフトウェアに対し誤動作させる要因を含んでいるか否かを判定し、前記誤動作させる要因を含んだ情報をもつ不正パケットであることを判定した際に、当該不正パケットを破棄し、正常なパケットと判定した受信パケットを前記第２のネットワークセグメントに送出することを特徴とする。

【００４７】また本発明の方法は、少なくとも第１及び第２のネットワークセグメントに接続され、前記第１及び第２のネットワークセグメント相互の間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送方法に於いて、前記第１のネットワークセグメントからのパケットを受信するステップと、前記受信した受信パケットに識別子を付加するステップと、前記識別子が付加された前記受信パケットを一時保留するステップと、前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定し、判定した正常な受信パケットの前記識別子を出力するステップと、前記識別子を受信し、前記一時保留されている前記受信パケットの中から、受信した前記識別子を持つ前記受信パケットを取り出し、前記第２のネットワークセグメントに送出するステップとを具備することを特徴とする。

【００４８】また本発明の方法は、少なくとも３つ以上のネットワークセグメントに接続され、複数の前記ネットワークセグメント間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送方法に於いて、前記ネットワークセグメントの一つからパケットを受信するステップと、前記受信した受信パケットに識別子を付加するステップと、前記識別子が付加された前記受信パケットを一時保留するステップと、前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定し、判定した正常な受信パケットの前記識別子を出力するステップと、前記識別子を受信し、前記一時保留されている前記受信パケットの中から、受信した前記識別子を持つ前記受信パケットを取り出し、当該受信パケットに含まれるＭＡＣアドレスから送出すべきネットワークセグメントを判定するステップと、前記判定されたネットワークセグメントに対し、取り出した前記受信パケットを送出するステップとを具備することを特徴とする。

【００４９】また本発明の方法は、少なくとも３つ以上のネットワークセグメントに接続され、複数の前記ネットワークセグメント間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送方法に於いて、前記ネットワークセグメントの一つからパケットを受信するステップと、前記受信した受信パケットに識別子を付加するステップと、前記識別子が付加された前記受信パケットに含まれる宛先ＭＡＣアドレスから当該受信パケットの送出

先ネットワークセグメントを判定し、前記送出先のネットワークセグメント毎に設けられた一時保留キューに、前記判定に従って前記受信パケットを格納するステップと、前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定し、判定した正常な受信パケットの前記識別子を出力するステップと、前記識別子を受信し、前記一時保留キューの前記受信パケットの中から、受信した前記識別子を持つ前記受信パケットを取り出し、対応するネットワークセグメントに送出するステップとを具備することを特徴とする。

【００５０】上記目的を達成するために、本発明のコンピュータ読み取り可能な記憶媒体は、少なくとも２つ以上のネットワークセグメント相互の間で転送されるパケットを監視するパケット転送装置に記憶され、前記ネットワークセグメントの一方からのパケットを受信する機能と、前記記受信した受信パケットに識別子を付加する機能と、前記識別子が付加された前記受信パケットを一時保留する機能と、前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定した際に、当該受信パケットの識別子を出力する機能と、前記識別子を受信し、前記一時保留されているパケットの中から受信した前記識別子を持つ受信パケットを取り出し、送出先の他方のネットワークセグメントへ送出する機能とを実現するためのプログラムが記憶される。

【００５１】また本発明の記憶媒体は、少なくとも３つ以上のネットワークセグメント間で転送されるパケットを監視するパケット転送装置に記憶され、前記ネットワークセグメントの一つからパケットを受信する機能と、前記受信した受信パケットに識別子を付加する機能と、前記識別子が付加された前記受信パケットを一時保留する機能と、前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定した際に、当該受信パケットの識別子を出力する機能と、前記識別子を受信し、前記一時保留されている受信パケットの中から受信した前記識別子を持つ受信パケットを取り出し、当該受信パケットに含まれるＭＡＣアドレスから送出すべきネットワークセグメントを判定する機能と、前記判定されたネットワークセグメントへ当該受信パケットを送出する機能とを実現するためのプログラムが記憶される。

【００５２】また本発明の記憶媒体は、少なくとも３つ以上のネットワークセグメント間で転送されるパケットを監視するパケット転送装置に記憶され、前記ネットワークセグメントの一つからパケットを受信する機能と、前記受信した受信パケットに識別子を付加する機能と、前記識別子が付加された前記受信パケットに含まれるＭＡＣアドレスから、送出すべきネットワークセグメントを判定する機能と、前記識別子が付加された前記受信パケットを、前記判定された送出先ネットワークセグメント毎に分けて一時保留する機能と、前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定した際に、当該受信パケットの識別子を出力する機能と、前記識別子を受信し、前記一時保留されている前記受信パケットの中から、受信した前記識別子を持つ受信パケットを取り出し、当該受信パケットを、前記判定された送出先ネットワークセグメントへ送出する機能とを実現するためのプログラムが記憶される。

【００５３】上記したような不正アクセスに関わるパケットを排除する機能をもつことにより、複数のネットワークセグメントに接続され、セグメント相互の間でパケットを転送するパケット転送装置に於いて、宛先／送信元ＭＡＣアドレスや、さらに上位のプロトコルの宛先／送信元アドレスやサービス番号等によってパケットを転送するか否かを判断するだけでは防止できない、不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。

【００５４】また、パケットを転送するか否かの判断を行なうための設定を利用者が行なうことなく、不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。

【００５５】また、ＩＰアドレス等のネットワークアドレスを全く持たないため、自身が不正アクセスの対象となることを防げる、不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。

【００５６】また、不正アクセスが為されていることを表示可能なパケット転送装置を実現することができる。

【００５７】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を説明する。

【００５８】先ず図１を参照して本発明の第１実施形態を説明する。

【００５９】図１は本発明の第１実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。この図１に示す第１実施形態では、パケット転送装置の片方向の転送についてのみ、不正アクセスに関わるパケットの通過を防ぐ機能を備えた構成を例示している。

【００６０】図１に示すパケット転送装置１０に於いて、パケット受信部１１と、パケット送出部１４は、それぞれ異なるネットワークセグメント（セグメントＡ－セグメントＢ）相互の間に接続される。ここではパケット受信部１１が接続されているネットワークセグメントＡから、パケット送出部１４が接続されているネットワークセグメントＢへパケットを転送する例を示している。

【００６１】パケット受信部１１は、ネットワークセグメントＡ上のパケットを受信する。パケット識別子付加機構１２は、受信したパケットに識別子を付加する。パ

ケット保留キュー１３は識別子を付加されたパケットを、パケット解析機構１５が、不正アクセスに関わるパケットで無いことを判定するまで一時保留する。パケット解析機構１５は、受信パケットを送出し、不正アクセスに関わるパケットで無いことを判定したパケットの識別子をパケット送出部１４に伝える。パケット送出部１４は、パケット解析機構１５から伝えられた識別子と同じ識別子が付加されている受信パケットをパケット保留キュー１３から取り出し、当該パケットをネットワークセグメントＢへ送出する。

【００６２】ここで、上記各図を参照して本発明の第１実施形態に於ける動作を説明する。

【００６３】図１に示すパケット転送装置１０に於いて、パケット受信部１１はネットワークセグメントＡに接続される送信側システム（又は端末、又は装置）から送信されたパケットを順次受信する。

【００６４】パケット識別子付加機構１２は、受信されたパケットに、装置内でユニークな識別子を付加する。この際の識別子としては、例えば、１，２，３，４と連番を付してゆく方法がある。また、パケットの到着時刻を用いる方法もある。あるいは、パケットを格納した記憶装置の番地を利用する方法もある。

【００６５】上記パケット識別子付加機構１２により識別子が付加されたパケットは、パケット保留キュー１３に格納されるとともに、パケット解析機構１５に渡される。

【００６６】パケット解析機構１５には、予め、不正アクセスに関わるパケットを識別するための判定情報が格納されているデータベース１５０が設けられる。このデータベース１５０には、少なくとも過去に受信した不正アクセスに関わるパケットに含まれていた文字列（判定情報）が格納されている。

【００６７】パケット識別子付加機構１２から受信パケットを渡されたパケット解析機構１５は、当該受信パケットをデータベース１５０に格納された判定情報に基づいて、不正アクセスに関わるか否かを判定する。データベース１５０には判定情報として、不正アクセスに関わるパケットに含まれる文字列の一覧が格納されている。パケット解析機構１５は、データベース１５０に格納された文字列一覧に含まれる文字列を受信パケットと逐次比較し、当該文字列一覧に含まれる文字列のいずれかが、受信パケットに含まれていた場合、当該受信パケットが不正アクセスに関わるものであると判定できる。受信パケットが不正アクセスに関わるものでは無いパケットであると判定した場合、パケット解析機構１５は、当該受信パケットに付加された識別子をパケット送出部１４に伝える。

【００６８】識別子を伝えられたパケット送出部１４は、パケット保留キュー１３から、当該識別子を持つ受信パケットを取り出し、ネットワークセグメントＢを介して受信側システム（又は端末、又は装置）に送出する。

【００６９】パケット解析機構１５に於いて、不正アクセスに関わるパケットであると判定された受信パケットは、パケット保留キュー１３に残され、明示的な指示あるいは、パケット保留キュー１３からの溢れによる等の暗黙的な手段によって破棄される。

【００７０】この一連の動作によって、不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。

【００７１】また、パケット解析機構１５のデータベース１５０に格納される、不正アクセスに関わるパケットを識別するための判定情報には、パケットデータの内容に関わるものをも含めることが可能であるため、宛先／送信元ＭＡＣアドレスや、さらに上位のプロトコルの宛先／送信元アドレスやサービス番号等によって、パケットを転送するか否かを判断するだけでは防止できない不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。

【００７２】また、このパケット解析機構１５のデータベース１５０に予め格納される、不正アクセスに関わるパケットを識別するための判定情報は、利用者や設置場所によらず、同一のものを利用可能であるため、利用者がパケットを転送するか否かの判断を行なうための設定を行なうこと無く不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。

【００７３】また、このパケット転送装置自身は、その動作を行なう上で、ＩＰアドレス等のネットワークアドレスを全く持つ必要が無いため、自身が不正アクセスの対象となることを防ぎ、不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。さらに、パケットデータの内容も、不正アクセスに関わるパケットを識別するための情報として利用することが可能であるため、明らかに不正アクセスに関わるパケットであるものを判定可能となる。例えば、アプリケーションプログラムに対して、規定より異常に長い文字列を送るようなパケットは、明らかに不正アクセスに関わるパケットであると判定できる。また、特定のデータ列が、アプリケーションプログラムやＯＳの誤動作を引き起こすことが知られている場合、当該データ列を含むパケットは、やはり、明らかに不正アクセスに関わるパケットであると判定できる。これらの、明らかに不正アクセスに関わるパケットであると判定できるパケットであると送出した場合に、利用者に表示することで、不正アクセスが成されていること、あるいは成されたことを表示可能なパケット転送装置を実現することができる。

【００７４】次に図２を参照して本発明の第２実施形態を説明する。

【００７５】図２は本発明の第２実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。

【００７６】この図２に示す第２実施形態では、パケット転送装置の両方向の転送について、不正アクセスに関わるパケットの通過を防ぐ機能を備えた構成を例示している。

【００７７】この図２に示すパケット転送装置２０は、ネットワークセグメントＡからネットワークセグメントＢへの不正アクセスに関わるパケットの通過を防ぐことができるとともに、ネットワークセグメントＢからネットワークセグメントＡへの不正アクセスに関わるパケットの通過を防ぐことができる。

【００７８】即ち、パケット転送装置２０に於いて、パケット受信部２１ａはネットワークセグメントＡより一つのパケットを受信する。

【００７９】パケット識別子付加機構２２ａは、受信されたパケットに、装置内でユニークな識別子を付加する。

【００８０】上記パケット識別子付加機構２２ａにより識別子が付加された受信パケットは、パケット保留キュー２３ａに格納されるとともに、パケット解析機構２５ａに渡される。パケット解析機構２５ａのデータベース２５０ａには、予め不正アクセスに関わるパケットを識別するための判定情報が格納されている。

【００８１】パケット識別子付加機構２２ａからパケットを渡されたパケット解析機構２５ａは、受信パケットをデータベース２５０ａに格納された判定情報に基づいて解析し、受信パケットが不正アクセスに関わるか否かを判定する。受信パケットが不正アクセスに関わるものでは無いパケットであると判定した場合、パケット解析機構２５ａは、当該受信パケットに付加された識別子をパケット送出部２４ｂに伝える。この識別子を受信したパケット送出部２４ｂは、パケット保留キュー２３ａから、当該識別子を持つ受信パケットを取り出し、ネットワークセグメントＢに送出する。

【００８２】パケット解析機構２５ａに於いて、不正アクセスに関わるパケットであると判定された受信パケットは、パケット保留キュー２３ａに残され、明示的な指示あるいは、パケット保留キュー２３ａからの溢れによる等の暗黙的な手段によって破棄される。

【００８３】一方、パケット受信部２１ｂはネットワークセグメントＢより一つのパケットを受信する。パケット識別子付加機構２２ｂは、受信したパケットに、装置内でユニークな識別子を付加する。

【００８４】上記パケット識別子付加機構２２ｂにより識別子が付加された受信パケットは、パケット保留キュー２３ｂに格納されるとともに、パケット解析機構２５ｂに渡される。パケット解析機構２５ｂのデータベース２５０ｂには、予め不正アクセスに関わるパケットを識別するための判定情報が格納されている。

【００８５】パケット識別子付加機構２２ｂから受信パケットを渡されたパケット解析機構２５ｂは、受信パケットをデータベース２５０ｂに格納された判定情報に基づいて解析し、受信パケットが不正アクセスに関わるか否かを判定する。受信パケットが不正アクセスに関わるものでは無いパケットであると判定した場合、パケット解析機構２５ｂは、当該受信パケットに付加された識別子をパケット送出部２４ａに伝える。

【００８６】識別子を伝えられたパケット送出部２４ａは、パケット保留キュー２３ｂから、当該識別子を持つ受信パケットを取り出し、ネットワークセグメントＡに送出する。

【００８７】パケット解析機構２５ｂに於いて、不正アクセスに関わるパケットであると判定された受信パケットは、パケット保留キュー２３ｂに残され、明示的な指示あるいは、パケット保留キュー２３ｂからの溢れによる等の暗黙的な手段によって破棄される。

【００８８】このような動作によって、ネットワークセグメントＡからネットワークセグメントＢへのパケット転送、およびネットワークセグメントＢからネットワークセグメントＡへのパケット転送について、その何れに於いても不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。

【００８９】次に図３を参照して本発明の第３実施形態を説明する。

【００９０】図３は本発明の第３実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。

【００９１】この図３に示す第３実施形態では、パケット転送装置の片方向の転送について、不正アクセスに関わるパケットの通過を防ぐ機能を備えた構成を例示している。

【００９２】この図３に示すパケット転送装置３０は、上記図２に示す第２実施形態の構成の簡素化を図ったもので、ネットワークセグメントＡからネットワークセグメントＢへの不正アクセスに関わるパケットに関してはその通過を防ぐが、ネットワークセグメントＢからネットワークセグメントＡへのパケット転送についてはパケットの通過を防げない構成としている。この図３に示す構成のパケット転送装置３０は、外部ネットワークとの接続点に設けられるような場合（例えばネットワークセグメントＢに接続されるシステムにおいて自己管理が可能な構内等のネットワークシステムであり、ネットワークセグメントＡが外界のネットワークシステムであるような場合）に、上記図２に示す第２実施形態に示すパケット転送装置２０に比して構成を簡素化できる。

【００９３】パケット転送装置３０に於いて、パケット受信部３１ａはネットワークセグメントＡより一つのパケットを受信する。パケット識別子付加機構３２は、パケット受信部３１ａからの受信パケットに対し、装置内でユニークな識別子を付加する。

【００９４】上記パケット識別子付加機構３２により識別子が付加された受信パケットは、パケット保留キュー

３３に格納されるとともに、パケット解析機構３５に渡される。パケット解析機構３５のデータベース３５０には、予め不正アクセスに関わるパケットを識別するための判定情報が格納されている。

【００９５】パケット識別子付加機構３２から受信パケットを渡されたパケット解析機構３５は、受信パケットをデータベース３５０に格納された識別情報に基づいて解析し、受信パケットが不正アクセスに関わるか否かを判定する。受信パケットが不正アクセスに関わるものでは無いパケットであると判定した場合、パケット解析機構３５は、当該受信パケットに付加された識別子をパケット送出部３４ｂに伝える。

【００９６】識別子を伝えられたパケット送出部３４ｂは、パケット保留キュー３３から、当該識別子を持つ受信パケットを取り出し、ネットワークセグメントＢに送出する。

【００９７】パケット解析機構３５に於いて、不正アクセスに関わるパケットであると判定されたパケットは、パケット保留キュー３３に残され、明示的な指示あるいは、パケット保留キュー３３からの溢れによる等の暗黙的な手段によって破棄される。

【００９８】一方、パケット受信部３１ｂはネットワークセグメントＢより一つのパケットを受信すると、当該パケットをそのまま（スルーモードで）パケット送出部３４ａに渡す。パケット送出部３４ａは、パケット受信部３１ｂより受けたパケットをネットワークセグメントＡに送出する。

【００９９】このような動作によって、ネットワークセグメントＡからネットワークセグメントＢへのパケット転送については、不正アクセスに関わるパケットを通過させることないよう厳重に管理され、逆方向の転送については不正アクセスに関する防御機能を簡略したパケット転送装置を実現することができる。

【０１００】次に図４、図５を参照して本発明の第４実施形態、および第５実施形態を説明する。

【０１０１】図４は、本発明の第４実施形態によるパケット転送装置の要部の構成要素を示すブロック図であり、図５は、本発明の第５実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。

【０１０２】この図４および図５に示す各実施形態では、何れに於いても、送出すべきネットワークセグメントを判定できた場合、判定されたネットワークセグメントのみに送出することで、判定されたネットワークセグメント以外のネットワークセグメントのトラフィックを削減することを可能にしている。

【０１０３】本発明に係るパケット転送装置が、３つ以上のネットワークセグメント間でパケットを転送する場合、あるネットワークセグメントから受信したパケットを、当該ネットワークセグメント以外の全てのネットワークセグメントに送出する方法がある。また、パケットの宛先ＭＡＣアドレスから、送出すべきネットワークセグメントを判定し、判定できた場合は、判定されたネットワークセグメントのみに送出することで、判定されたネットワークセグメント以外のネットワークセグメントのトラフィックを削減する方法もある。

【０１０４】図４に示す第４実施形態では、各送出セグメントに対して、パケット保留キューを共通としたパケット転送装置４０の構成を示している。ここでは、パケット解析機構４５により、パケットが不正アクセスに関わるか否かを判定した後に、送出すべきネットワークセグメントを判定する構成としている。

【０１０５】上記図４に示す構成のパケット転送装置４０に於いて、パケット受信部４１により受信され、パケット識別子付加機構４２によって識別子が付加された受信パケットは、全ての送出セグメントに共通のパケット保留キュー４３に格納される。

【０１０６】パケット解析機構４５はデータベース４５０に格納された判定情報に基づき、受信パケットが不正アクセスに関わるか否かを判定し、不正アクセスに関わるパケットでは無いと判定した場合、当該受信パケットの識別子を送出セグメント判定機構４６に通知する。

【０１０７】パケット解析機構４５より識別子を通知された送出セグメント判定機構４６は、当該識別子を持つ受信パケットをパケット保留キュー４３から取り出し、受信パケットの宛先ＭＡＣアドレスから、送出すべきネットワークセグメントを識別し、識別できた場合は、判定されたネットワークセグメントに対応する少なくとも一つのパケット送出部（４４ａ～４４ｎのいずれか）に受信パケットを受け渡す。そして、パケット送出部は識別したネットワークセグメントに受信パケットを送出する。また、ネットワークセグメントが識別できなかった場合は、全てのパケット送出部４４ａ～４４ｎに受信パケットが送られ、パケット送出部４４ａ～４４ｎに接続されるネットワークセグメントに受信パケットが送出される。

【０１０８】図５に示す第５実施形態では、送出ネットワークセグメントそれぞれに固有のパケット保留キューを設けたパケット転送装置５０の構成を示している。ここでは、パケット解析機構５５により受信パケットが不正アクセスに関わるか否かを判定する以前に、送出すべきネットワークセグメントを判定する構成としている。

【０１０９】図５において、パケット受信部５１に受信され、パケット識別子付加機構５２によって識別子が付加された受信パケットは、送出セグメント判定機構５６およびパケット解析機構５５に渡される。

【０１１０】送出セグメント判定機構５６は、パケット受信部５１で受信され、パケット識別子付加機構５２によって識別子が付加された受信パケットの宛先ＭＡＣアドレスから、送出すべきネットワークセグメントを識別し、その識別したネットワークセグメントに対応するパ

ケット保留キュー（５３ａ～５３ｎのいずれか）に当該受信パケットを格納する。

【０１１１】パケット保留キュー５３ａ～５３ｎは、送出セグメント判定機構５６によって格納された受信パケットを、パケット解析機構５５によって不正アクセスに関わるパケットで無いことが判定されるまで一時保留する。そして、このパケット保留キュー５３ａ～５３ｎに対応してパケット送出部５４ａ～５４ｎがそれぞれ接続されている。

【０１１２】パケット解析機構５５は、データベース５５０に格納された判定情報に基づき、受信パケットが不正アクセスに関わるか否かを判定し、受信パケットが不正アクセスに関わるパケットでは無いと判定した場合、当該受信パケットの識別子をパケット送出部５４ａ～５４ｎに通知する。

【０１１３】パケット解析機構５５より識別子を通知されたパケット送出部５４ａ～５４ｎは、当該識別子を持つ受信パケットが対応して接続されているパケット保留キュー５３ａ～５３ｎに存在するとき、当該受信パケットを取り出し、対応するネットワークセグメントに送出する。

【０１１４】また、送出セグメント判定機構５６は、送出すべきネットワークセグメントが認識できなかった場合は、受信パケットを全てのパケット保留キュー５３ａ～５３ｎに格納する。そして、受信パケットがパケット解析機構５５より不正アクセスではないと判定され、当該受信パケットの識別子がパケット送出部５４ａ～５４ｎに通知された時、パケット送出部５４ａ～５４ｎはパケット保留キュー５３ａ～５３ｎから受信パケットを取り出し、対応する全てのネットワークセグメントにそのパケットを送出する。

【０１１５】このような構成とすることにより、パケット解析機構５５で不正アクセスに関わるパケットでは無いと判定されてからパケット送出部（５４ａ～５４ｎ）へ送出されるまでの時間が短縮できる効果がある。

【０１１６】そして、上記した第４実施形態、第５実施形態によれば、送出すべきネットワークセグメントを識別できた場合は、識別されたネットワークセグメントのみにパケットの送出を行なうことで、識別されたネットワークセグメント以外のネットワークセグメントのトラフィックを削減することが可能となる。

【０１１７】次に、図６乃至図８を参照して本発明の第６実施形態を説明する。

【０１１８】図６は、本発明の第６実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。図７および図８は、それぞれ第６実施形態に於ける不正アクセス表示手段の例を示す図である。

【０１１９】この図６に示す第６実施形態のパケット転送装置６０は、パケット解析機構６５が不正アクセスに関わるパケットであるという判定した受信パケットの存在、構造、形式、受信時刻、送信元の少なくともいずれかを含む詳細情報を不正アクセス履歴として記録し表示する機能を備えている。

【０１２０】不正アクセス履歴保持機構６６は、パケット解析機構６５が不正アクセスに関わるパケットであるという判定した受信パケットについて、その存在、および受信時刻、送信元等の詳細情報をパケット解析機構６５より取得し、保持する。

【０１２１】不正アクセス履歴表示機構６７は、不正アクセス履歴保持機構６６が保持する不正アクセス履歴を表示するものである。この際の不正アクセス履歴表示機構６７の具体例を図７、図８にそれぞれ示している。

【０１２２】上記図６に示す構成のパケット転送装置６０に於いて、パケット識別子付加機構６２は、パケット受信部６１で受信された受信パケットに、装置内でユニークな識別子を付加する。

【０１２３】上記パケット識別子付加機構６２により識別子が付加された受信パケットは、パケット保留キュー６３に格納されるとともに、パケット解析機構６５に渡される。

【０１２４】パケット識別子付加機構６２から受信パケットを渡されたパケット解析機構６５は、データベース６５０に格納された判定情報に基づき解析し、当該受信パケットが不正アクセスに関わるか否かを判定する。

【０１２５】したがって、パケット解析機構６５はパケット受信部６１を介して不正アクセスに関わるパケットが受信されると、当該受信パケットが不正アクセスであると判定する。この際、パケット解析機構６５は、当該受信パケットの識別子をパケット送出部６４へ送出せず、不正アクセスに関わるパケットが受信側ネットワークセグメントに転送されないことは上記した各実施形態と同様である。

【０１２６】この第６実施形態に於いては、上記パケット解析機構６５が不正アクセスに関わるパケットであると判定した際、不正アクセス履歴保持機構６６に不正アクセスの存在、並びに受信時刻や送信元、送信先、不正の種類などの情報を不正アクセス履歴情報として送出する。

【０１２７】不正アクセス履歴保持機構６６は、上記パケット解析機構６５より取得した不正アクセス履歴を保持し、利用者が不正アクセス履歴の消去の作業を行なうまでそれを保持する。

【０１２８】不正アクセス履歴表示機構６７は、不正アクセス履歴保持機構６６に保持されている、不正アクセスに関わるパケットの存在、受信時刻、送信元、送信先、およびパケット解析機構６５が判定した不正の種類等の不正アクセス履歴情報の内容を表示する。

【０１２９】この際の不正アクセス履歴表示機構６７の具体的な構成例としては、図７に示すのように、パケット転送装置６０の筐体に設けられた、例えばＬＥＤ等を

用いた不正アクセス表示器６７Ａを点灯駆動して、不正アクセスの存在を利用者に報知する構成とする。または、図８に示すように、不正アクセスの時刻、送信元、送信先、不正の種類などを例えばＬＣＤ等を用いた不正アクセス表示装置６７Ｂに文字表示して、利用者に、不正アクセスの時刻、送信元、送信先、不正の種類などの詳細情報を報知する構成とする。さらに、履歴情報を遡って表示するためのスイッチを備えて、利用者が、不正アクセスの履歴情報を遡って確認できるようにすることもできる。

【０１３０】次に、図９乃至図１２を参照して本発明の第７実施形態を説明する。

【０１３１】図９は、本発明の第７実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。

【０１３２】この図９に示す第７実施形態のパケット転送装置７０は、複数のパケットが必要なパケットの解析時に参照される送出済みのパケットを保持する送出済みパケット保持機構７６を具備したことを特徴とする。

【０１３３】送出済みパケット保持機構７６は、パケット解析機構７５が受信パケットを送出する際に参照されるもので、パケット解析機構７５が解析処理した送出済みのパケットを保持する機能をもつ。

【０１３４】パケット解析機構７５は、パケット受信部７１がパケットを受信し、パケット識別子付加機構７２が識別子を付加した受信パケットを解析する際に、当該受信パケットに加えて、当該受信パケット以前に送出した送出済みパケットをあわせて参照し、不正アクセスに関わるパケットであるか否かを判定する。

【０１３５】上記図９に示す構成のパケット転送装置７０に於いて、パケット受信部７１で受信され、パケット識別子付加機構７２により識別子が付加された受信パケットは、パケット保留キュー７３に格納され、パケット解析機構７５に渡されると同時に送出済みパケット保持機構７６に保持される。

【０１３６】パケット解析機構７５は、パケット識別子付加機構７２から渡された受信パケットを送出する際に、装置内に組み込まれた後述するパケット解析プログラムによる判定情報（他の実施形態と同様にデータベースを参照しても良い）、および送出済みパケット保持機構７６に保持されている当該受信パケット以前に送出したパケットを含めて参照（この参照では、過去に正常なパケットと判定したことを示す）し、パケット識別子付加機構７２から渡された受信パケットが不正アクセスに関わるパケットであるか否かを判定する。

【０１３７】パケット解析機構７５は、パケット解析プログラムの解析に基づいて、受信パケットが不正アクセスに関わるパケットであると判定した場合、送出済みパケット保持機構７６に保持されている当該受信パケット（不正アクセスのパケット）を破棄する。これにより、以降の解析において、送出したパケットのみを参照することとなり、より正確な解析を可能とする。

【０１３８】送出済みパケット保持機構７６に、保持されているパケットを、例えば、格納してから一定期間過ぎたら破棄する方法や、宛先毎に予め指定した特定のデータ量を越えたら、越えた分、到着順序に従い破棄する方法などによって、送出済みパケット保持機構７６に新しいパケットが格納できなくなることを防ぐ機構が設けられる。

【０１３９】また、送出済みパケット保持機構７６に、パケット解析機構７５からの送出済みパケットの参照が容易となるように、例えば、特定の宛先へのパケットのみを取り出す機能や、パケットに含まれる連番の順にパケットを並び替えて取り出す機能が設けられる。これにより、アプリケーションプログラムやＯＳ等に対してバグを引き起こすことが知られている特定のデータ列が、複数のパケットに跨って送られてきた場合など、受信パケットをそれぞれ別個に判定しては見逃してしまうような不正アクセスに関わるパケットであっても見つけることが可能となる。

【０１４０】図１０は、上述したパケット解析プログラムを用いたパケット解析機構の構成例を示すブロック図である。ここでは、図９に示す第７実施形態に於けるパケット解析機構７５を例にとって示しているが、上述した第１乃至第６の実施形態に示した不正パケット解析用データベースの変わりに、パケット解析機構を適用しても良い。

【０１４１】図１０に示すパケット転送装置のパケット解析機構７５は、実行プログラムの形式で不正アクセスに関わるパケットの判定を行う処理機能が実現される。

【０１４２】図１０に示すパケット解析機構７５に於いて、パケット格納部７５１は、命令実行機構７５４からメモリ制御機構７５３を介してアクセスされる記憶装置であり、パケット識別子付加機構７２により識別子が付加された受信パケットや、送出済みパケット保持機構７６に保持されている送出済みパケットが格納される。

【０１４３】実行命令格納部７５２は、命令実行機構７５４が動作するのに必要なパケット解析プログラムを格納する記憶装置である。

【０１４４】メモリ制御機構７５３は、命令実行機構７５４からのアクセス要求に基づき、パケット格納部７５１、あるいは実行命令格納部７５２、あるいはその他の記憶装置と命令実行機構７５４との間で、格納されたデータを受け渡す機能を持つ。

【０１４５】命令実行機構７５４は、メモリ制御機構７５３から渡されるパケット解析プログラムに従い、パケット格納部７５１に格納されたパケットが、不正アクセスに関わるパケットであるか否かを判定するためのパケット解析処理を実行する。

【０１４６】この命令実行機構７５４の実行結果によ

り、受信パケットが不正アクセスに関わるパケットであるか否かが判定される。そして、当該受信パケットが不正アクセスに関わるパケットで無い場合は、当該受信パケットを送出すべく、パケット送出部７４（あるいは図４、図５に示す送出セグメント判定機構４６，５６）に、当該受信パケットの識別子が伝えられる。

【０１４７】ここで、図１０に示す構成のパケット解析機構７５に於ける処理動作を、図９に示すパケット転送装置７０を適用した場合を基に説明する。

【０１４８】図１０に示す構成のパケット解析機構７５に於いて、実行命令格納部７５２には、命令実行機構７５４が動作するのに必要なパケット解析プログラムが予め格納されている。

【０１４９】図９に示すパケット転送装置７０に於いて、パケット受信部７１で受信されたパケットはパケット識別子機構７２によって識別子が付加される。この識別子が付加された受信パケットは、パケット保留キュー７３に格納され、またパケット解析機構７５に渡されると同時に、送出済みパケット保持機構７６にも格納される。パケット解析機構７５に渡されたパケットは、パケット格納部７５１に格納される。

【０１５０】パケット格納部７５１に受信パケットを格納する方法としては、パケット識別子付加機構７２、または送出済みパケット保持機構７６から受信パケットをコピーしてくる方法。または、パケット識別子付加機構７２や送出済みパケット保持機構７６と記憶装置（パケット格納部７５１）を共有する方法等がある。送出済みパケット保持機構７６を持つ場合、送出済みパケット保持機構７６に保持されている送出済みパケットもパケット格納部７５１に格納する構成にしてもよい。

【０１５１】パケット格納部７５１へのパケットの格納が完了すると、命令実行機構７５４の動作が開始される。命令実行機構７５４は、メモリ制御機構７５３を介して実行命令格納部７５２に格納されたパケット解析プログラム（実行プログラム）を先頭から逐次読み出して送出処理を実行する。

【０１５２】例えば、パケット格納部７５１に格納された受信パケットに、不正アクセスに関わるパケットに含まれる文字列が含まれているか否かを解析する場合、実行命令格納部７５２に格納されたパケット解析プログラムの一部には、不正アクセスに関わるパケットに含まれる文字列の一覧が含まれており、命令実行機構７５４は、メモリ制御機構７５３を介して、当該文字列一覧に含まれる文字列と受信パケットを逐次比較して、当該文字列一覧に含まれる文字列のいずれかが受信パケットに含まれていた場合、当該受信パケットが不正アクセスに関わるものであると判定する。

【０１５３】また、命令実行機構７５４は、実行命令格納部７５２に格納されたパケット解析プログラムに従い、送出済みパケット保持機構７６が持つ、例えば特定の宛先への受信パケットのみを取り出す機能や、受信パケットに含まれる連番順にパケットを並び替えて取り出す機能等を利用して、送出済みパケット保持機構７６から送出済みのパケットを取り出し、パケット格納部７５１に格納する機能を持つこともできる。

【０１５４】命令実行機構７５４はパケット解析プログラムの終端まで処理を実行し、受信パケットが不正アクセスに関わるものであるか否かを判定する。

【０１５５】このような不正アクセスに関わるパケットの判定機能をもつ構造とすることで、例えば、ＯＳの誤動作を引き起こすことが知られている特定のデータ列として、一部のみ異なる複数のデータ列がある場合、共通する部分の比較は一度で完了することが可能となり、不正アクセスに関わるものであるか否かの判定をより高速に行なうことが可能となる。さらに、命令実行機構７５４の動作が停止している期間に、実行命令格納部７５２の実行プログラムを入れ替えると、次のパケットを受信した際に、新しく入れ替えられた実行プログラムにしたがって、解析が開始されることから、パケット解析機構７５の不正アクセスの解析手段を更新することも容易となる。

【０１５６】図１１及び図１２のフローチャートは、実行命令格納部７５２に格納されるパケット解析プログラムを命令実行機構７５４が実行して、不正アクセスに関わるパケットの判定処理の具体例な処理手順を示す。

【０１５７】この図１１及び図１２に示す判定処理では、上記パケット格納部７５１に格納された受信パケットについて、先ずヘッダフィールドのオプションや、パラメータの組み合わせがパケット転送先のサーバに誤動作を引き起こすとして予め設定された既知の条件を満たしているか否かが判定される（図１１ステップＳ１１）。即ち、受信パケットのヘッダ部から不審な相手からの送信であったり、形式の異なる怪しいパケットであることを見分ける処理を行なう。

【０１５８】ここで上記条件を満たしていれば、当該受信パケットは破棄の対象となる（図１１ステップＳ１５）。一方、上記条件を満たしていなければ、次に、断片化されたパケットやＴＰＣ等、判断に他のパケットの情報も必要となるか否かが判断される（図１１ステップＳ１２）。

【０１５９】他のパケットを必要としない場合は、次にパケットが搬送しているデータの長さ、あるいはデータが指定しているパラメータの組み合わせが、そのデータを処理するアプリケーションに誤動作を引き起こすとして予め設定された既知の条件を満たしているか否かが判定される（図１１ステップＳ１３）。

【０１６０】ここで上記条件を満たしていれば当該受信パケットは破棄の対象となる（図１１ステップＳ１５）。一方、上記条件を満たしていなければ、当該受信パケットを送出対象パケットとして、パケット送出部７

４に当該受信パケットの転送指示を行う（図１１ステップＳ１４）。

【０１６１】また、上記ステップＳ１２に於いて、他のパケットの情報も必要であると判断された際は、断片化されたパケットで、かつ送出済みパケット保持機構７６から取り出した他の断片化されたパケットとデータ領域がオーバーラップしている等、サーバに誤動作引き起こすとして予め設定された既知の条件を満たしているか否かが判定される（図１２ステップＳ２１）。

【０１６２】ここで上記条件を満たしていれば当該受信パケットは破棄の対象となる（図１２ステップＳ２６）。一方、上記条件を満たしていなければ、次に、ＴＰＣのパケットで、送出済みパケット保持機構７６から取り出した同一セッションの他のパケットとデータ領域がオーバーラップしている等、サーバに誤動作引き起こすとして予め設定された既知の条件を満たしているか否かが判定される（図１２ステップＳ２２）。

【０１６３】ここで上記条件を満たしていれば当該受信パケットは破棄の対象となる（図１２ステップＳ２６）。一方、上記条件を満たしていなければ、次に、送出済みパケット保持機構７６から必要に応じた数の同一セッションのパケットを取り出し、送出に充分な長さのデータストリームを再構築し（図１２ステップＳ２３）、当該ＴＣＰデータストリームによって搬送されているデータの長さ、あるいはデータが指定しているパラメータは誤動作を引き起こすとして予め設定された既知の条件を満たしているか否かが判定される（図１２ステップＳ２４）。

【０１６４】ここで上記条件を満たしていれば当該受信パケットは破棄の対象となる（図１２ステップＳ２６）。一方、上記条件を満たしていなければ、パケット送出部７４に当該受信パケットの転送指示を行う（図１２ステップＳ２５）。

【０１６５】このような不正アクセスに関わるパケットの判定処理が、パケット受信部７１で受信した各受信パケットについて順次実行される。

【０１６６】上記したような不正アクセスに関わるパケットを排除する機能をもつことにより、宛先／送信元ＭＡＣアドレスや、さらに上位のプロトコルの宛先／送信元アドレスやサービス番号等によってパケットを転送するか否かを判断するだけでは防止できない、不正アクセスに関わるパケットを通過させないパケット転送機構が実現できる。またパケットを転送するか否かの判断を行なうための設定を利用者が行なうことなく不正アクセスに関わるパケットを通過させないパケット転送機構を実現できる。またＩＰアドレス等のネットワークアドレスを全く持たないため、自身が不正アクセスの対象となることを防げる、不正アクセスに関わるパケットを通過させないパケット転送機構が実現できる。

【０１６７】尚、上記した実行命令格納部７５２に格納される実行プログラム（パケット送出プログラム）は、例えばハードディスク、ＣＤ－ＲＯＭ、半導体メモリ等の各種記憶媒体または記憶装置により提供することも可能である。

【０１６８】次に、図１３を参照して本発明の第８実施形態を説明する。

【０１６９】図１３は、本発明の第８実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。

【０１７０】この図１３に示す第７実施形態のパケット転送装置８０は、シリアルインタフェース８７を介してパケット解析プログラムを更新する機能を付加したことを特徴とする。

【０１７１】図１３に示すパケット転送装置８０に於いて、パケット解析機構８５の実行命令格納部８６には、命令実行機構（図１０を参照）が動作するための実行プログラムが格納されている。

【０１７２】シリアルインタフェース８７は、外部からの解析プログラム更新指示を受信する機能を持つ。解析プログラム更新機構８８は、シリアルインタフェース８７が受信した解析プログラム更新指示に従って、パケット解析機構８５に格納された実行プログラムを更新する機能を持つ。更新指示形式識別機構８９は、シリアルインタフェース８７で受信したデータが、解析プログラム更新指示であるか否かを、当該受信したデータが特定の形式を満たしているか否かによって判定する機能を持つ。

【０１７３】上記図１３に示すパケット転送装置８０の動作を説明する。

【０１７４】シリアルインタフェース８７を介して受信されたデータは解析プログラム更新機構８８に渡される。解析プログラム更新機構８８は、更新指示形式識別機構８９によって、シリアルインタフェース８７から渡されたデータが特定の形式を満たしている解析プログラム更新指示であることを確認すると、当該解析プログラム更新指示に含まれている実行プログラムを取り出す。

【０１７５】更に、解析プログラム更新機構８８は、パケット解析機構８５の命令実行機構が動作中か否かを確認し、動作中の場合は、動作が停止するのを待つ。パケット解析機構８５の命令実行機構が停止していることを確認した場合、解析プログラム更新指示に含まれる実行プログラムをパケット解析機構８５の実行命令格納部８６に格納する。これにより、パケット解析機構８５内の不正アクセスを解析する実行プログラムが更新される。

【０１７６】次に、図１４を参照して本発明の第９実施形態を説明する。

【０１７７】図１４は、本発明の第９実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。

【０１７８】この図１４に示す第９実施形態のパケット

転送装置９０は、ネットワークインタフェース９７を介してパケット解析プログラムを更新する機能を付加したことを特徴とする。この第９の実施形態は、図１３の実施形態のシリアルインタフェース８７がネットワークインタフェース９７に置き換わったものであり、その他の構成は図１３と同じであるためその説明は省略する。

【０１７９】次に、図１４に示すパケット転送装置９０の動作を説明する。

【０１８０】ネットワークインタフェース９７を介して受信されたデータは解析プログラム更新機構９８に渡される。解析プログラム更新機構９８は、更新指示形式識別機構９９によって、ネットワークインタフェース９７から渡されたデータが特定の形式を満たしている解析プログラム更新指示であることを確認すると、当該解析プログラム更新指示に含まれている実行プログラムを取り出す。

【０１８１】更に、解析プログラム更新機構９８は、パケット解析機構９５の命令実行機構が動作中か否かを確認し、動作中の場合は、動作が停止するのを待つ。パケット解析機構９５の命令実行機構が停止していることを確認した場合、解析プログラム更新指示に含まれる実行プログラムをパケット解析機構９５の実行命令格納部９６に格納する。これにより、パケット解析機構９５内の不正アクセスを解析する実行プログラムが更新される。

【０１８２】次に、図１５を参照して本発明の第１０実施形態を説明する。

【０１８３】図１５は、本発明の第１０実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。

【０１８４】この図１５に示す第１０実施形態のパケット転送装置１００は、パケットを利用して実行プログラム（パケット解析プログラム）を更新する機能を付加したことを特徴とする。

【０１８５】図１５に示すパケット転送装置１００に於いて、パケット解析機構１０５の実行命令格納部１０６には、命令実行機構（図１０を参照）が動作するための実行プログラムが格納されている。

【０１８６】解析プログラム更新機構１０７は、パケット受信部１０１によって受信された解析プログラム更新指示に従って、パケット解析機構１０５に格納された実行プログラムを更新する機能を持つ。解析プログラム更新機構１０７内の更新指示形式識別機構１０８は、入力されたパケットのデータが特定の形式を満たしているか否かによって、受信パケットが解析プログラム更新指示であるか否かを判定する機能を持つ。

【０１８７】次に、図１５に示すパケット転送装置１００の動作を説明する。

【０１８８】パケット受信部１０１で受信されたパケットは、パケット識別子付加機構１０２に渡されるのと同時に、解析プログラム更新機構１０７に渡される。解析プログラム更新機構１０７の更新指示形式識別機構１０８は、入力された受信パケットが解析プログラム更新指示を示す特定の形式を満たしていることを判定する。特定の形式を満たしている場合、その受信パケットは転送されるべきパケットでは無く、解析プログラム更新指示であると判断する。これにより、解析プログラム更新機構１０７は当該受信パケットに含まれる実行プログラムを取り出して、パケット解析機構１０５に送り、実行命令格納部１０６に格納される。

【０１８９】上記した図１３乃至図１５に示す各実施形態は、何れもパケット解析機構の実行命令格納部に格納される実行プログラムを更新して、最新の不正アクセス解析プログラムが稼動する環境を整えるものであるが、不正な解析プログラム更新指示によって、不正アクセス解析プログラムが不正に更新されてしまい、パケット解析機構が正常に動作しないようにされてしまう可能性がある。

【０１９０】これを防ぐために、図１６に示すように、更新指示形式識別機構に、電子署名識別機構を備え、解析プログラム更新指示に、電子署名を付加して認証することも可能である。尚、ここでは図１５に示す第１０実施形態を対象にしているが、図１３に示す第８実施形態、図１４に示す第９実施形態に於いても同様に適用可能である。

【０１９１】図１６は、解析プログラム更新機構１０７の構成を示すブロック図であり、ここでは、解析プログラム更新機構１０７内に更新指示形式識別機構１０８と、更新指示形式識別機構１０８内に電子署名識別機構１０９を備える構成としている。

【０１９２】即ち、更新指示形式識別機構１０８内の電子署名識別機構１０９は、シリアルインタフェース（図１３）や、ネットワークインタフェース（図１４）から受信したデータや、パケット受信部（図１５）で受信されたパケットに格納されているデータ中に含まれている電子署名が正当な署名であるか否かを判定する。即ち、解析プログラム更新指示を示すデータが、特定の形式を満たしており、かつ当該データ中に含まれている電子署名が正当な署名である場合に、正当な解析プログラム更新指示であると判定する。

【０１９３】解析プログラム更新機構１０７は、更新指示形式識別機構１０８が、正当な解析プログラム更新指示であると判定した場合、その解析プログラム更新指示に含まれる不正アクセス解析プログラムをパケット解析機構１０５に出力する機能を有する。

【０１９４】上記の構成において、解析プログラム更新機構１０７に渡されたデータが、解析プログラム更新指示であることを示す特定の形式を満たしており、かつ、電子署名識別機構１０９によって当該データ中に含まれている電子署名が正当な署名である場合、解析プログラム更新機構１０７は正当な解析プログラム更新指示であ

ると判定し、そのデータに含まれる不正アクセス解析プログラムを取り出して、パケット解析機構１０５に送り、パケット解析機構１０５は実行命令格納部１０６に不正アクセス解析プログラムを格納する。これにより、不正な解析プログラム更新指示によって、パケット解析機構が正常に動作しないようにされてしまうことを防げるパケット転送装置を実現することができる。

【０１９５】次に、図１７を参照して本発明の第１１実施形態を説明する。

【０１９６】図１７は、本発明の第１１実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。この第１１実施形態のパケット転送装置１１０は、通信用アドレスを予め設定する機能をもつことを特徴とする。

【０１９７】図１７に示すパケット転送装置１１０に於いて、通信用アドレス設定機構１１４は、シリアルインタフェースやネットワークインタフェース等を介して得られる通信用アドレスを、通信用アドレス保持機構１１５に設定する機能を持つ。この図１７に示す例では、シリアルインタフェース１１３を介して通信用アドレスを設定する場合を例に示している。

【０１９８】通信用アドレス保持機構１１５は、通信用アドレス設定機構１１４によって予め設定された通信用アドレスを保持する機能を持つ。

【０１９９】通信制御機構１１２は、パケット解析プログラムの更新に伴う通信や、装置内情報通知機構１１７がネットワークセグメントに接続される他の装置に対して通知するための通信（以下、これらの通信を特定通信と称する）を制御する装置であり、上記特定通信を行なわないときは、上記通信アドレス宛のパケットは破棄する機能を持つ。また、上記特定通信を行なうときには、上記通信アドレス宛のパケットを受信し、当該パケットに格納された当該特定通信に関わるデータを実行プログラム更新機構１１６や装置内情報通知機構１１７へ渡す機能を持つ。また、上記特定通信に関わるデータ通信時に、実行プログラム更新機構１１６や装置内情報通知機構１１７が送信するデータに当該通信アドレスを送信元として付加してネットワークセグメントへ送出する機能を持つ。

【０２００】この実施形態のパケット転送装置１１０には、例えば、図６に示す不正アクセス履歴保持機構６６に保持されている不正アクセス履歴や、その他の装置内部の情報を外部に通知するための装置内情報通知機構１１７を持たせている。装置内情報通知機構１１７は、装置内部の情報を外部へ通知するのに、シリアルインタフェースや、通知用ネットワークインタフェースを利用する。また、装置内情報通知機構１１７は、装置内部の情報を外部に通知するのに、パケット転送の対象である、パケット受信部／パケット送出部が接続されたネットワークセグメントを利用することもできるが、その場合、自身が不正アクセスの対象となることを防ぐために通常動作中は持っていない、ネットワークアドレスが必要となる。

【０２０１】次に、図１７に示すパケット転送装置１１０の動作を説明する。

【０２０２】利用者は、通信用アドレス設定機構１１４を利用して、通信用アドレス保持機構１１５に、通信用アドレスを予め設定しておく。図１７の構成では、シリアルインタフェース１１３を介して通信用アドレス設定機構１１４を利用する場合を示しているが、ネットワークインタフェースを利用したり、解析プログラム更新指示と同様の方法で、転送対象のネットワークセグメントを介して、通信用アドレス設定機構１１４を利用することも可能である。

【０２０３】上記特定通信を行なう場合、通信制御機構１１２は、ネットワークセグメントからパケット受信部１１１を介して当該通信アドレス宛のパケットが送信されてきた場合、これを受信し、その受信パケットに含まれる通信に関わるデータを実行プログラム更新機構１１６や装置内情報通知機構１１７へ渡す。そして、実行プログラム更新機構１１６や装置内情報通知機構１１７は特定通信に関わる送信データを、上記通信アドレス宛によって示される送信元のネットワークセグメントへ送出する。しかしながら、通信を行なわないときは、通信制御機構１１２が上記通信アドレス宛のパケットを破棄し、自身が不正アクセスの対象となることを防ぐ。

【０２０４】次に、図１８および図１９を参照して本発明の第１２実施形態を説明する。

【０２０５】図１８は、本発明の第１２実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。この図１８に示す第１２実施形態のパケット転送装置１２０は、パケット横奪部１２２を持つ構成としたことを特徴とする。

【０２０６】図１８に示すパケット転送装置１２０に於いて、通信用アドレス選択機構１２４は、過去に受信したパケットのネットワークアドレスと受信したネットワークセグメントとの対応を保持するアドレス／セグメント対応表１２５を持ち、上記特定通信に関わるパケットの送出先ネットワークセグメントとは異なるネットワークセグメントから、過去に受信したパケットの送信元アドレスのうちの任意の１つを通信用アドレスとして選択し、その選択した通信用アドレスを通信用アドレス保持機構１２６に設定する機能を持つ。

【０２０７】この際のアドレス／セグメント対応表１２５の一例を図１９に示している。

【０２０８】通信用アドレス保持機構１２６は、通信用アドレス選択機構１２４によって設定された通信用アドレスを保持する機能を持つ。

【０２０９】パケット横奪部１２２は、上記特定通信を行なわないときは、通信アドレス宛のパケットをパケッ

ト識別子付加機構（図１乃至図６を参照）に渡して、通常の転送処理を行ない、上記特定通信を行なうときは通信アドレス宛のパケットをパケット識別子付加機構に渡さずに横奪する機能を持つ。

【０２１０】通信制御機構１２３は、上記特定通信を制御する機構であり、受信パケットに含まれる通信に関わるデータを実行プログラム更新機構１２７や、装置内情報通知機構１２８へ渡す。また、実行プログラム更新機構１２７や装置内情報通知機構１２８が送信するデータに、当該通信アドレスを送信元として付加してネットワークセグメントへ送出する機能を持つ。

【０２１１】次に、図１８に示すパケット転送装置１２０の動作を説明する。

【０２１２】通信用アドレス選択機構１２４は、内蔵するアドレス／セグメント対応表１２５を参照して、特定通信に関わるパケットの送出先となるネットワークセグメントから、過去に受信したパケットの送信元アドレスの１つを通信用アドレスとして選択する。

【０２１３】ここで、アドレス／セグメント対応表１２５に保持された、アドレスと受信したネットワークセグメントの対応が、例えば図１９に示す内容であるとする。ここで、上記特定通信を行なう相手が、［１９２．１６８．７．４２］のネットワークアドレスを持っているとすると、上記特定通信に関わるパケットを送出すべきネットワークセグメントはセグメントＢであることが判る。

【０２１４】したがって、上記特定通信に関わるパケットを送出すべきネットワークセグメント（セグメントＢ）と異なるネットワークセグメントとはセグメントＡであり、通信用アドレスとしては、［１９２．１６８．０．２１］、あるいは［１９２．１６８．３．１３４］のいずれかを選択すれば良いこととなる。

【０２１５】例えば、アドレス／セグメント対応表１２５の先頭に最も近いセグメントＡを選択するとすると、アドレスは［１９２．１６８．０．２１］となる。この際、もしも、上記特定通信を行なう相手のネットワークアドレスが、アドレス／セグメント対応表１２５に存在しなかった場合は、各々のネットワークセグメント上のアドレスを任意に選択し、そのアドレスを用いてアドレス設定を行う。このアドレス設定の結果、いずれかのネットワークセグメント上で、アドレス設定の応答パケットを受信できると、アドレス／セグメント対応表１２５に当該通信を行なう相手のネットワークアドレスとネットワークセグメントが登録されるので、改めて当該ネットワークアドレスを通信用アドレスとして選択する。

【０２１６】通信用アドレスをこのように選択することで、当該通信アドレスが指定されている応答パケットがパケット転送装置１２０のパケット受信部１２１に送信される。パケット横奪部１２２は、上記特定通信を行なわないときは、セグメントＡの通信アドレス宛のパケットは、パケット識別子付加機構に渡して通常の転送処理を行なう。一方、上記特定通信を行なうときは、セグメントＡの通信アドレス宛のパケットを横奪して、当該通信用アドレスの本来の持ち主にパケットが渡らないようにする。

【０２１７】パケット横奪部１２２は、通信制御機構１２３が送出したパケットに対するネットワークセグメントからの応答パケットのみを横奪することで、当該通信用アドレスの本来の持ち主の通信への影響を最小限にすることも可能である。この場合、当該通信用アドレスの本来の持ち主の通信と区別ができるように、当該通信用アドレスの本来の持ち主が、この実施形態によるパケット転送装置１２０を経由する通信で用いているポート番号等を保存しておき、当該装置の通信時は、それらと重ならないようにして当該通信用アドレスの本来の持ち主の通信と区別できるようにする等の仕組みを用意する必要がある。このようにすることで、自身への不正アクセスを防ぎつつ、解析プログラムの更新に伴う通信や、装置内情報通知機構が他の装置に対して装置内部の情報を通知するための特定通信が可能となる。

【０２１８】上記した図１７、若しくは図１８に示した各実施形態の構造をもつことによって、解析プログラムの更新に伴う通信や、装置内情報通知機構が他の装置に対して装置内部の情報を通知するための通信、等の特定の通信を行なっているとき以外は、ネットワークアドレスを持たないため、自身への不正アクセスを防げるパケット転送装置を実現することができる。

【０２１９】次に、図２０および図２１を参照して本発明の第１３実施形態を説明する。

【０２２０】図２０は、本発明の第１３実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。この図２０に示す第１３実施形態のパケット転送装置１３０は、通信開始指示形式識別機構１３３を具備することを特徴とする。

【０２２１】通信開始指示形式識別機構１３３は、パケット受信部１３１で受信されたパケットが、通信開始指示を示す特定の形式を満たしているデータであることを識別して、通信制御機構１３４に通信開始を通知する機能を持つ。

【０２２２】通信制御機構１３４は、通信開始指示形式識別機構１３３からの通信開始の通知を受けると、通信用アドレス保持機構１３６に保持された通信用アドレス、あるいは通信用アドレス選択機構１３５が選択した通信用アドレスを用いた通信を開始する機能を持つ。

【０２２３】次に、図２０に示すパケット転送装置１３０の動作を説明する。

【０２２４】上記した図１７および図１８に示す各実施形態の構造によって、上記特定通信を行なっているとき以外は、ネットワークアドレスを持たないパケット転送装置を実現した場合、上記実施形態のパケット転送装置

から他の装置に対して通信を開始することが可能であるが、他の装置から上記実施形態のパケット転送装置へ対する通信を開始しようとしても、ネットワークアドレスを持たないため、通信が不可能である。そこで、この図２０に示す第１３実施形態のパケット転送装置１３０では、他の装置からパケット転送装置１３０に対する通信を開始することができるようにするため、通信開始指示形式識別機構１３３を持つ。

【０２２５】パケット受信部１３１で受信されたパケットは、パケット識別子付加機構（図１乃至図６など参照）等に渡されるのと同時に、通信開始指示形式識別機構１３３にも渡される。通信開始指示形式識別機構１３３は、受信したパケットの形式が、通信開始指示を示す特定の形式を満たしているか否かを判定する。

【０２２６】特定の形式を満たしている場合、受信したパケットは、ネットワークセグメントに送出されるべきパケットでは無く、パケット転送装置１３０に対する通信開始指示であると判断し、通信制御機構１３４は通信開始を指示する。この図２０に示す例では、通信制御機構１３４が通信用アドレス選択機構１３５で選択した通信用アドレスを用いて通信を開始すると想定する。

【０２２７】このようにすることで、解析プログラムの更新に伴う通信や、装置内情報通知機構１３８が他の装置に対して装置内部の情報を通知するための通信、等でなる特定通信を行なっているとき以外は、パケット転送装置１３０はネットワークアドレスを持たないため、自身への不正アクセスを防ぐことができ、かつ他の装置からパケット転送装置１３０に対する通信を開始することが可能なパケット転送機能を実現することができる。

【０２２８】上記した実施形態に於いては、外部から通信を開始する機能を持つ場合、不正な通信開始指示によって通信を開始され、自身が不正アクセスの対象とされてしまう可能性がある。これを防ぐために、図２１に示すように、通信開始指示形式識別機構１３３に、電子署名識別機構１３９を備え、通信開始指示に、電子署名を付加して認証することも可能である。

【０２２９】図２１に示すように、通信開始指示形式識別機構１３３内には電子署名識別機構１３９が設けられ、この電子署名識別機構１３９は通信開始指示のデータ中に含まれている電子署名が正当な署名であるか否かを判定して、電子署名が正当な署名である場合に、当該データは正当な通信開始指示であると判定し、通信制御機構１３４に通信開始を通知する。

【０２３０】通信制御機構１３４は、通信開始指示形式識別機構１３３から通信開始の通知を受けると、通信用アドレス保持機構１３６に保持された通信用アドレス、あるいは通信用アドレス選択機構１３５が選択した通信用アドレスを用いた通信を開始する。

【０２３１】これにより、不正な通信開始指示によって、通信を開始され、自身が不正アクセスの対象とされてしまうことを防げるパケット転送装置を実現することができる。

【０２３２】尚、上記した図１３乃至図２０に示す各実施形態に於いて扱われるパケット解析プログラムは、例えばハードディスク、ＣＤ－ＲＯＭ、半導体メモリ等の各種記憶媒体または記憶装置により装置個々に個別に提供することも可能である。

【０２３３】上記したような本発明の実施形態により、宛先／送信元ＭＡＣアドレスや、さらに上位のプロトコルの宛先／送信元アドレスやサービス番号等によってパケットを転送するか否かを判断するだけでは防止できない、不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。また、パケットを転送するか否かの判断を行なうための設定を利用者が行なうことなく、不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。また、ＩＰアドレス等のネットワークアドレスを全く持たないため、自身が不正アクセスの対象となることを防げる、不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。また、不正アクセスが為されていることを表示可能なパケット転送装置を実現することができる。

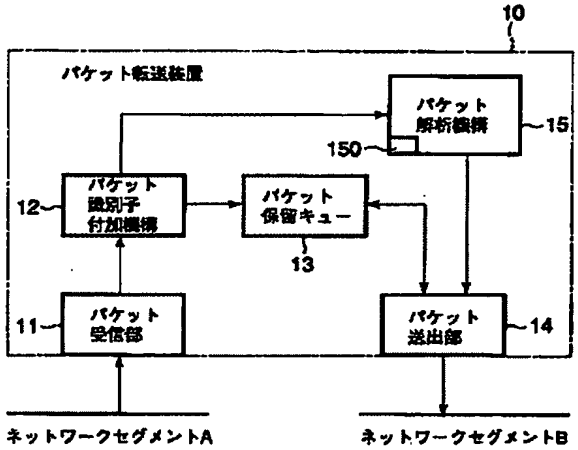
【０２３４】更に、上記した実施形態の機能を、図２２乃至図２４を参照して説明した既存の不正アクセス防止機能と組み合わせることで、より信頼性の高い不正アクセスに関わるパケットの転送防止機能を実現することができる。

【０２３５】

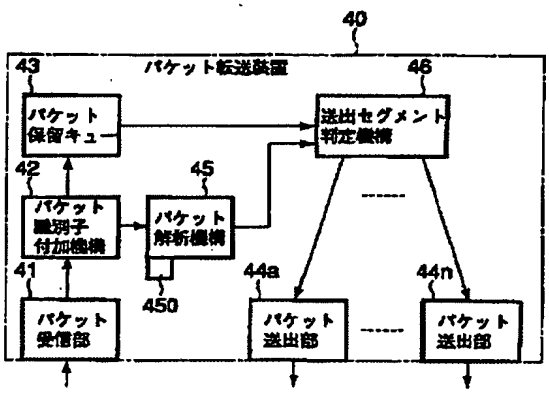
【発明の効果】以上詳記したように本発明によれば、利用者に大きな作業負担をかけることなく、信頼性の高い不正アクセスの防止機能を実現できる。更に本発明によれば、送信元より転送されたパケットの内容を送出して不正アクセスに関わるパケットでないことを判定する機能をもつことで、不正アクセスに関わるパケットの転送を確実に防止でき、信頼性の高い不正アクセスの防止機能が実現できる。即ち本発明によれば、宛先／送信元ＭＡＣアドレスや、さらに上位のプロトコルの宛先／送信元アドレスやサービス番号等によってパケットを転送するか否かを判断するだけでは防止できない、不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。またパケットを転送するか否かの判断を行なうための設定を利用者が行なうことなく不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。またＩＰアドレス等のネットワークアドレスを全く持たないため、自身が不正アクセスの対象となることを防ぐことのできる、不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。更に不正アクセスが為されていることを表示可能なパケット転送装置を実現することができる。

【図面の簡単な説明】
【図１】本発明の第１実施形態によるパケット転送装置の要部の構成要素を示すブロック図。
【図２】本発明の第２実施形態によるパケット転送装置の要部の構成要素を示すブロック図。
【図３】本発明の第３実施形態によるパケット転送装置の要部の構成要素を示すブロック図。
【図４】本発明の第４実施形態によるパケット転送装置の要部の構成要素を示すブロック図。
【図５】本発明の第５実施形態によるパケット転送装置の要部の構成要素を示すブロック図。
【図６】本発明の第６実施形態によるパケット転送装置の要部の構成要素を示すブロック図。
【図７】上記第６実施形態に於ける不正アクセス表示手段の第１の例を示す図。
【図８】上記第６実施形態に於ける不正アクセス表示手段の第２の例を示す図。
【図９】本発明の第７実施形態によるパケット転送装置の要部の構成要素を示すブロック図。
【図１０】上記第７実施形態に於けるパケット解析機構の構成例を示すブロック図。
【図１１】上記第７実施形態に於ける不正アクセスに関わるパケットの判定処理の処理手順を示すフローチャート。
【図１２】上記第７実施形態に於ける不正アクセスに関わるパケットの判定処理の処理手順を示すフローチャート。
【図１３】本発明の第８実施形態によるパケット転送装置の要部の構成要素を示すブロック図。
【図１４】本発明の第９実施形態によるパケット転送装置の要部の構成要素を示すブロック図。
【図１５】本発明の第１０実施形態によるパケット転送装置の要部の構成要素を示すブロック図。
【図１６】上記第１０実施形態に於ける解析プログラム更新機構の構成を示すブロック図。
【図１７】本発明の第１１実施形態によるパケット転送装置の要部の構成要素を示すブロック図。
【図１８】本発明の第１２実施形態によるパケット転送装置の要部の構成要素を示すブロック図。
【図１９】上記第１２実施形態に於けるアドレス／セグメント対応表の構成例を示す図。
【図２０】本発明の第１３実施形態によるパケット転送装置の要部の構成要素を示すブロック図。
【図２１】上記第１３実施形態に於ける通信開始識別機構の他の構成例を示すブロック図。
【図２２】従来のパケット転送装置の構成を示すブロック図。
【図２３】上記図２２に示す従来のパケット転送装置のネットワーク構成例を示すブロック図。
【図２４】上記図２３に示す従来のパケット転送装置のルール保持部に格納される内容例を示す図。
【符号の説明】
１０，２０，３０，４０，５０，６０，７０，８０，９０，１００，１１０，１２０，１３０…パケット転送装置
１１，２１ａ，２１ｂ，３１ａ，３１ｂ，４１，５１，６１，７１，８１，９１，１０１，１１１，１２１，１３１…パケット受信部
１２，２２ａ，２２ｂ，３２，４２，５２，６２，７２，８２，９２，１０２…パケット識別子付加機構
１３，２３ａ，２３ｂ，３３，４３，５３ａ…５３ｎ，６３，７３，８３，９３，１０３，…パケット保留キュー
１４，２４ａ，２４ｂ，３４ａ，３４ｂ，４４ａ…４４ｎ，５４ａ…５４ｎ，６４，７４，８４，９４，１０４，…パケット送出部
１５，２５ａ，２５ｂ，３５，４５，５５，６５，７５，８５，９５，１０５…パケット解析機構
１５０，２５０ａ，２５０ｂ，３５０，４５０，５５０，６５０…不正パケット解析用データベース
４６，５６…送出セグメント判定機構
６６…不正アクセス履歴保持機構
６７…不正アクセス履歴表示機構
６７Ａ…不正アクセス表示器
６７Ｂ…不正アクセス表示装置
７６…送出済みパケット保持機構
８６，９６，１０６…実行命令格納部
８７，１１３…シリアルインタフェース
８８，９８，１０７…解析プログラム更新機構
８９，９９，１０８…更新指示形式識別機構
９７…ネットワークインタフェース
１０９，１３９…電子署名識別機構
１１２，１２３，１３４…通信制御機構
１１４…通信用アドレス設定機構
１１５，１２６，１３６…通信用アドレス保持機構
１１６，１２７，１３７…実行プログラム更新機構
１１７，１２８，１３８…装置内情報通知機構
１２２，１３２…パケット横奪部
１２４，１３５…通信用アドレス選択機構
１２５…アドレス／セグメント対応表
１３３…通信開始指示形式識別機構
７５１…パケット格納部
７５２…実行命令格納部
７５３…メモリ制御機構
７５４…命令実行機構

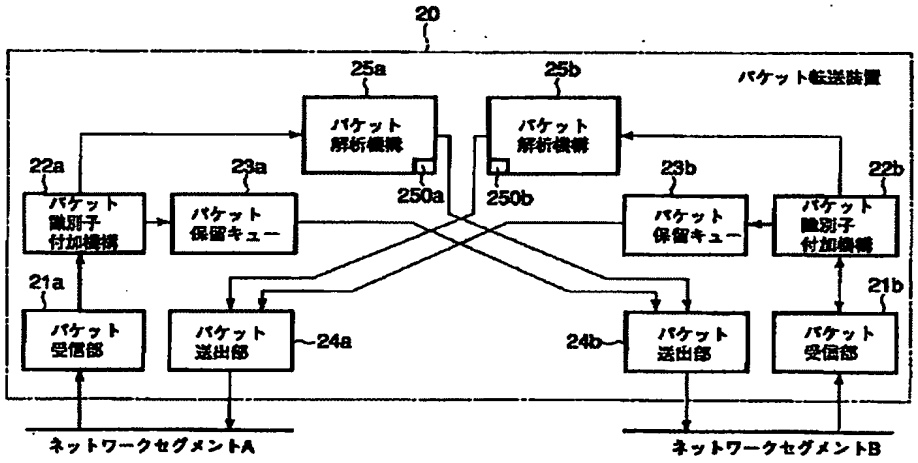
【図１】


10
パケット転送装置
パケット解析機構
15
150
パケット識別子付加機構
12
パケット保留キュー
13
パケット受信部
11
パケット送出部
14
ネットワークセグメントA
ネットワークセグメントB

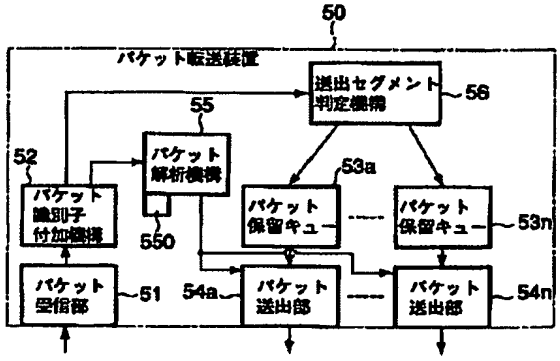
【図４】


40
43
パケット転送装置
46
パケット保留キュー
送出セグメント判定機構
42
45
パケット識別子付加機構
パケット解析機構
41
450
44a
44n
パケット受信部
パケット送出部
パケット送出部

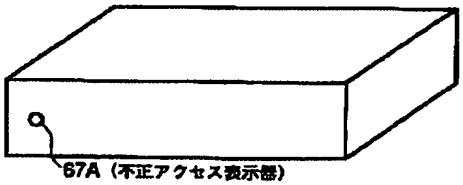
【図２】


20
25a
25b
パケット転送装置
パケット解析機構
パケット解析機構
22a
23a
250a
250b
23b
22b
パケット識別子付加機構
パケット保留キュー
パケット保留キュー
パケット識別子付加機構
21a
21b
パケット受信部
パケット送出部
24a
24b
パケット送出部
パケット受信部
ネットワークセグメントA
ネットワークセグメントB

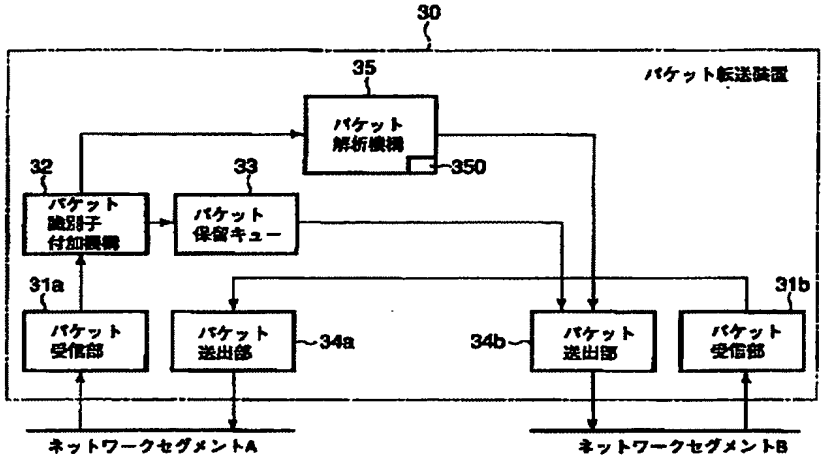
【図５】


50
パケット転送装置
送出セグメント判定機構
56
55
52
パケット解析機構
53a
パケット識別子付加機構
パケット保留キュー
パケット保留キュー
53n
550
パケット受信部
51
54a
パケット送出部
パケット送出部
54n

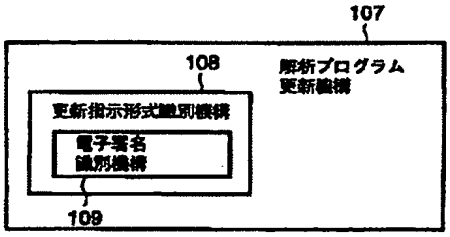
【図７】


67A（不正アクセス表示器）

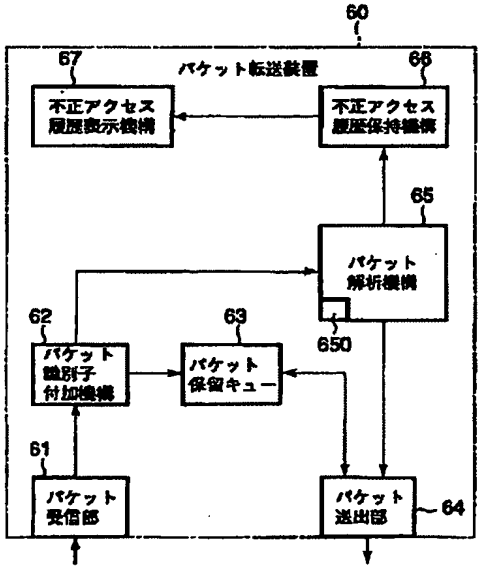
【図３】



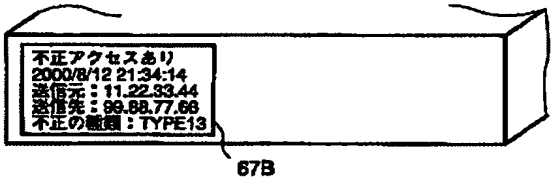
【図１６】



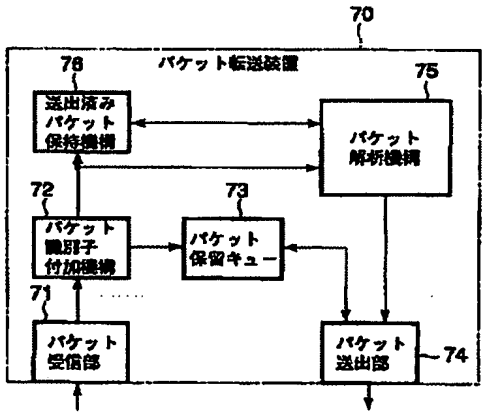
【図６】



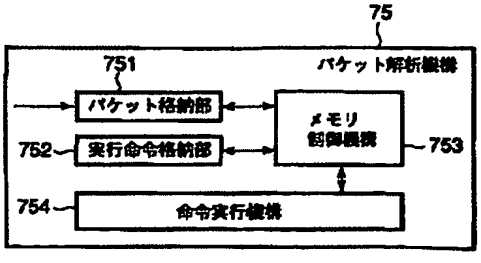
【図８】



【図９】



【図１０】

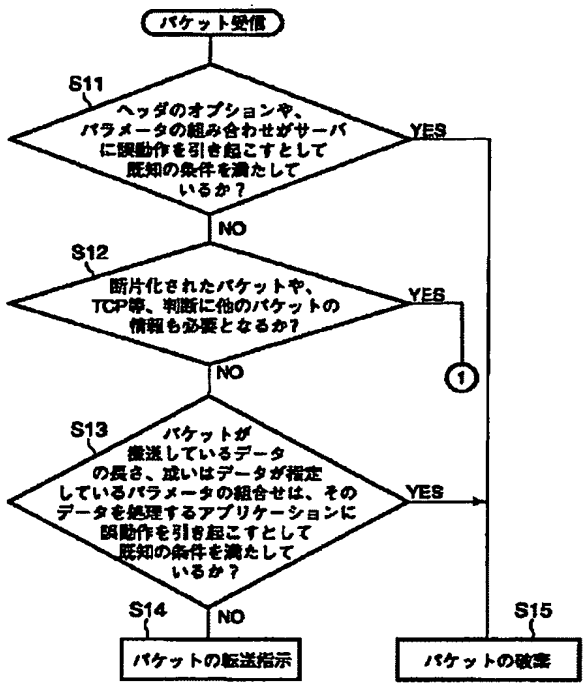


【図１９】

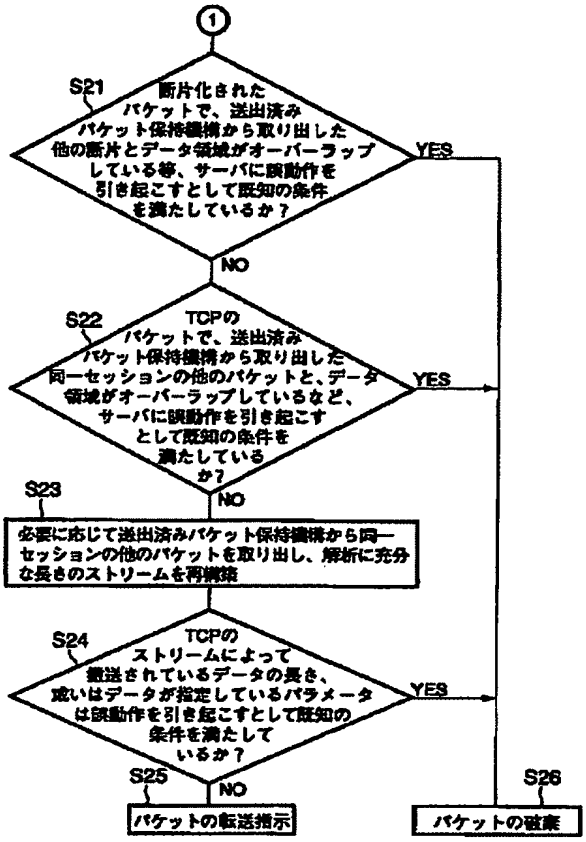
アドレス	受信したネットワークセグメント
192.168.0.21	セグメントA
192.168.1.17	セグメントB
192.168.1.232	セグメントB
192.168.3.134	セグメントA
192.168.7.42	セグメントB

125

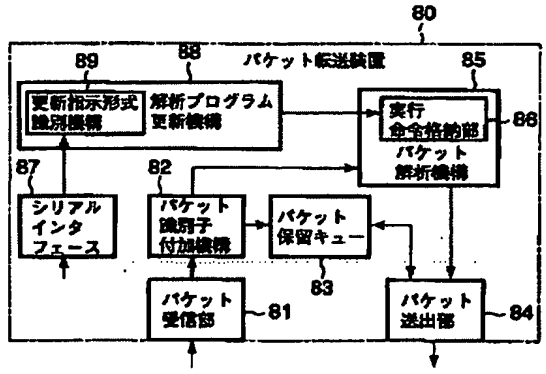
【図１１】



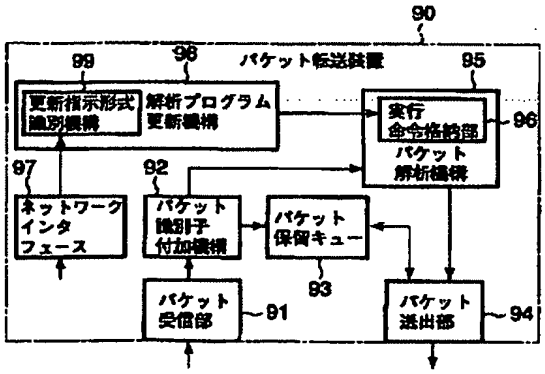
【図１２】



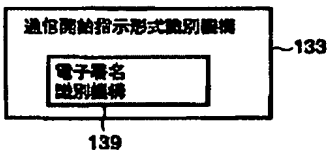
【図１３】



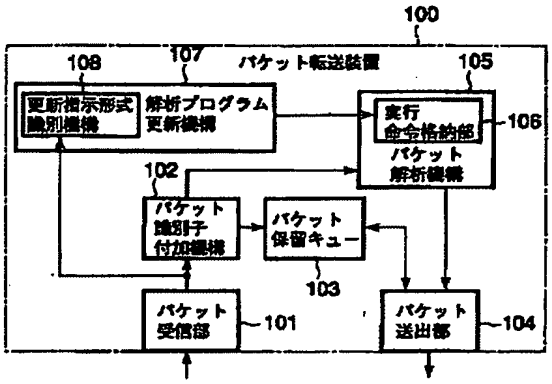
【図１４】



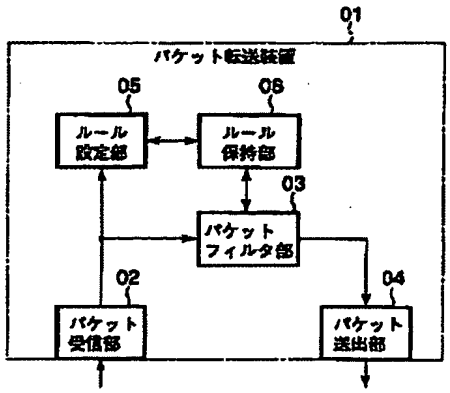
【図２１】



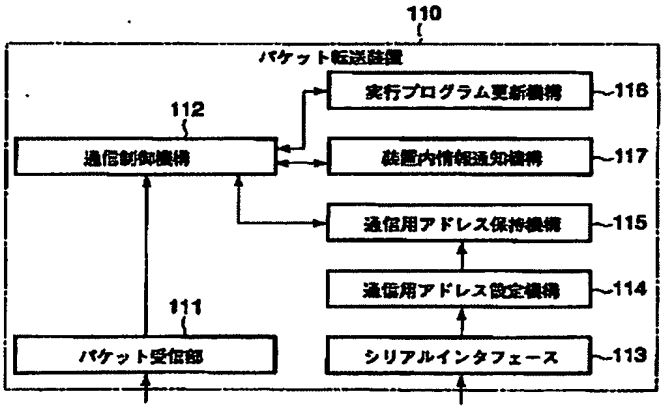
【図１５】



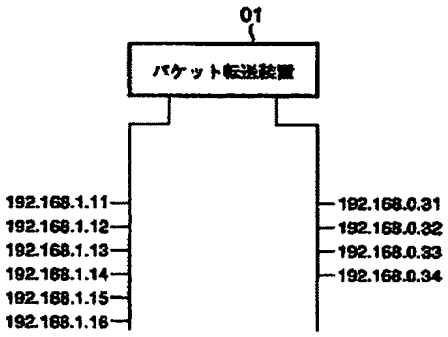
【図２２】



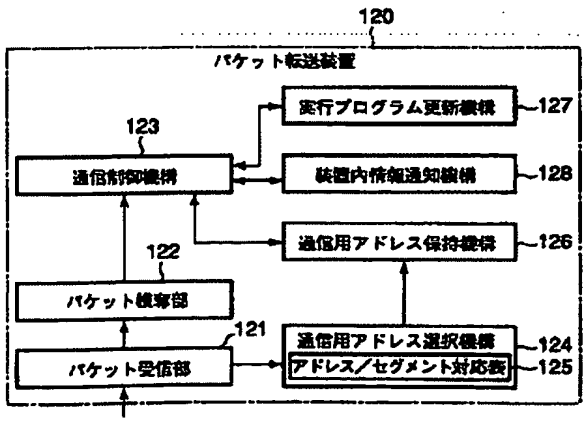
【図１７】



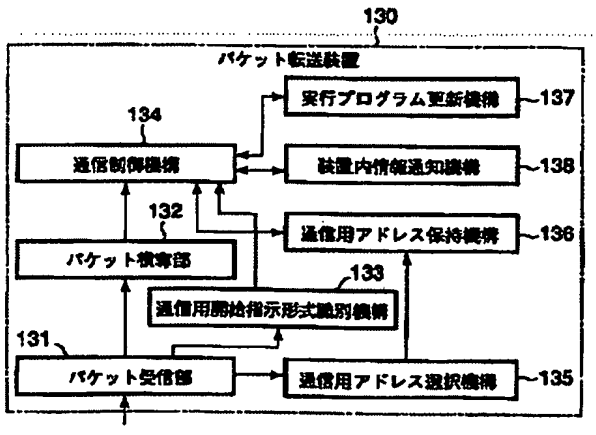
【図２３】



【図１８】



【図２０】



【図２４】

宛先	送信元	宛先	転送許可
192.168.0.31	192.168.1.11	HTTP	許可
192.168.0.31	192.168.1.12	HTTP	許可
192.168.0.31	192.168.1.13	HTTP	不許可
192.168.0.31	192.168.1.14	HTTP	不許可
192.168.0.31	192.168.1.11	SMTP	許可
192.168.0.31	192.168.1.12	SMTP	不許可
192.168.0.31	192.168.1.13	SMTP	不許可
192.168.0.31	192.168.1.14	SMTP	許可
192.168.0.33	any	HTTP	許可
any	192.168.1.15	HTTP	不許可
any	192.168.1.16	SMTP	許可

06